1016 B Y4.G74/7:C73/26/985

COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

ORIGINAL

MFQL

COMPLETED

126

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON
GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST SESSION

ON

H.R. 2889

TO AMEND THE ACT ESTABLISHING THE NATIONAL BUREAU OF STANDARDS TO PROVIDE FOR A COMPUTER SECURITY RESEARCH PROGRAM WITHIN SUCH BUREAU, AND TO PROVIDE FOR THE TRAINING OF FEDERAL EMPLOYEES WHO ARE INVOLVED IN THE MANAGEMENT, OPERATION, AND USE OF AUTOMATED INFORMATION PROCESSING SYSTEMS

SEPTEMBER 18, 1985

Printed for the use of the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE
51-589 O WASHINGTON : 1985

I

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

DON FUQUA, Florida
JOHN CONYERS, Jr., Michigan
CARDISS COLLINS, Illinois
GLENN ENGLISH, Oklahoma
HENRY A. WAXMAN, California
TED WEISS, New York
MIKE SYNAR, Oklahoma
STEPHEN L. NEAL, North Carolina
DOUG BARNARD, Jr., Georgia
BARNEY FRANK, Massachusetts
TOM LANTOS, California
ROBERT E. WISE, Jr., West Virginia
BARBARA BOXER, California
SANDER M. LEVIN, Michigan
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, Jr., South Carolina
JOE KOLTER, Pennsylvania
BEN ERDREICH, Alabama
GERALD D. KLECZKA, Wisconsin
ALBERT G. BUSTAMANTE, Texas
MATTHEW G. MARTINEZ, California

FRANK HORTON, New York
THOMAS N. KINDNESS, Ohio
ROBERT S. WALKER, Pennsylvania
WILLIAM F. CLINGER, Jr., Pennsylvania
ALFRED A. (AL) McCANDLESS, California
LARRY E. CRAIG, Idaho
HOWARD C. NIELSON, Utah
JIM SAXTON, New Jersey
PATRICK L. SWINDALL, Georgia
THOMAS D. (TOM) DeLAY, Texas
JOHN J. DioGUARDI, New York
JOHN G. ROWLAND, Connecticut
RICHARD K. ARMEY, Texas
JIM LIGHTFOOT, Iowa
JOHN R. MILLER, Washington
——— ———

William M. Jones, *General Counsel*
John E. Moore, *Staff Administrator*
James E. Lewin, *Chief Investigator*
Stephen M. Daniels, *Minority Staff Director and Counsel*

Legislation and National Security Subcommittee

JACK BROOKS, Texas, *Chairman*

DON FUQUA, Florida
HENRY A. WAXMAN, California
STEPHEN L. NEAL, North Carolina
TOM LANTOS, California
JOHN CONYERS, Jr., Michigan

FRANK HORTON, New York
JIM SAXTON, New Jersey
JOSEPH J. DioGUARDI, New York
JOHN G. ROWLAND, Connecticut

Richard C. Barnes, *Staff Director*

CONTENTS

Page

Hearing held on September 18, 1985 1

Text of H.R. 2889 3

Statement of:

- Brooks, Hon. Jack, a Representative in Congress from the State of Texas, and chairman, Legislation and National Security Subcommittee: Opening statement 1
- Brown, Clarence J., Deputy Secretary, U.S. Department of Commerce, accompanied by Raymond G. Kammer, Jr., Deputy Director, National Bureau of Standards 24
- Burrows, James H., Director, Institute for Computer Sciences and Technology, National Bureau of Standards 29
- Glickman, Hon. Dan, a Representative in Congress from the State of Kansas 9
- Latham, Donald C., Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, Department of Defense 47
- Rich, Robert E., Deputy Director, National Security Agency, accompanied by Walter Deeley, Deputy Director, Communications and Computer Security; Elizabeth Rindskopf, General Counsel; and Col. Joseph Greene, Assistant to the Director for Computer Security 64
- Socolar, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office, accompanied by William Franklin, Associate Director, Defense Management and Support Systems, Information Management and Technology Division, and Gary Kepplinger, Acting Assistant General Counsel, Special Studies and Analysis, Office of the General Counsel 13

Letters, statements, et cetera, submitted for the record by:

- Burrows, James H., Director, Institute for Computer Sciences and Technology, National Bureau of Standards: Prepared statement 35-44
- Latham, Donald C., Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, Department of Defense:
  - Companies currently on the main advisory committee to the NSTAC.. 61
  - National security sensitive information 49-50
  - Prepared statement 52-56
- Rich, Robert E., Deputy Director, National Security Agency: Prepared statement 65-71
- Socolar, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office: Prepared statement 16-20

APPENDIXES

Appendix 1.—National Security Decision Directive 145 73

Appendix 2.—Statements submitted for the record 83

COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

WEDNESDAY, SEPTEMBER 18, 1985

House of Representatives,
Legislation and National Security Subcommittee
of the Committee on Government Operations,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2154, Rayburn House Office Building, Hon. Jack Brooks (chairman of the subcommittee) presiding.

Present: Representatives Jack Brooks, Stephen L. Neal, Frank Horton, and John G. Rowland.

Subcommittee staff present: Richard C. Barnes, staff director; and Mary Alice Oliver, clerk; full committee staff: William M. Jones, general counsel; John E. Moore, staff administrator; James E. Lewin, chief investigator; James E. Rife, Charles C. Wheeler III, and Robert S. Richard, professional staff members; Ralph Doty, staff member; Stephen M. Daniels, minority staff director and counsel; Douglas D. Mitchell, and Gregg Kilgore, minority professional staff, Committee on Government Operations.

OPENING STATEMENT OF CHAIRMAN BROOKS

Mr. Brooks. The subcommittee will come to order.

The hearing is called to consider H.R. 2889, the Computer Security Research and Training Act of 1985. This legislation was introduced by Congressman Dan Glickman in June and subsequently referred jointly to the Committees on Science and Technology and Government Operations.

Congressman Fuqua, chairman of the Science and Technology Committee, Congressman Horton, and myself are strong supporters of the bill and are among the original cosponsors.

H.R. 2889 establishes a new research program within the National Bureau of Standards [NBS], to assess the vulnerability of Government computers and communications. It also provides for the development of technical and management techniques to defend against unlawful access to sensitive Government information. Further, Federal agencies would be required to provide mandatory training for their employees in computer and communications security.

In my view, this legislation is long overdue. Over the years, this subcommittee has conducted extensive investigations of computer and communications facilities of several major Federal agencies.

We found that in almost every case security was lax or virtually nonexistent.

One of the most disturbing things we found was that the lack of interim controls and automatic audit checks makes it likely that once a perpetrator gains access to the computer system, the agency may never even be aware of it. In spite of this, computer and communications security has remained a low priority for most Federal agencies and a relatively small amount of funds are devoted to this area.

While everyone appears to support the need for increased security, there is no general consensus within the executive branch or the Congress on how best to accomplish this.

Late last year, the President issued National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security." Under this directive, DOD was given the authority to issue policies and standards for the safeguarding of not only classified information, but other information in the civilian agencies and the private sector which it believed to be sensitive. This apparent expansion of DOD's authorities raised considerable congressional and public concern.

Some of these concerns, including my own, were explored during Congressman Glickman's hearings in June of this year. I have asked today's witnesses to provide their views on the directive and how a better balance may be struck between the need to safeguard information and the need to maintain a free exchange of information in an open society. In my view, this balance can be struck, and I am hoping that this legislation will become the vehicle to achieve this end.

[The bill, H.R. 2889, follows:]

I

99TH CONGRESS
1ST SESSION

H. R. 2889

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

IN THE HOUSE OF REPRESENTATIVES

JUNE 27, 1985

Mr. GLICKMAN (for himself, Mr. FUQUA, Mr. BROOKS, Mr. BROWN of California, Mr. WIRTH, Mr. WALGREN, Mr. NELSON of Florida, Mr. WYDEN, Mr. HUGHES, Mr. LEWIS of Florida, and Mr. HORTON) introduced the following bill; which was referred jointly to the Committees on Science and Technology and Government Operations

---

A BILL

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Research and Training Act of 1985".

SEC. 2. FINDINGS.

The Congress finds that—

(1) in recent years the Federal Government has become highly dependent on automated information processing systems for carrying out many of its missions;

(2) the Government operates about 20,000 medium- and large-scale mainframe computers, and by the end of this decade it will also have approximately half a million micro- and mini-computers;

(3) the information stored in Government computers and transmitted over the various communications networks that connect them represent valued property that is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption;

(4) studies of computer-related fraud and abuse in Government agencies indicate a costly and widespread problem of significant proportions;

(5) Government efforts to address the problems of computer security have focused on developing hardware and software systems to protect sensitive information, ensuring that new computer systems are designed to include security provisions, and requiring agencies to implement security procedures; and

(6) these efforts must be supplemented if the problems are to be solved, since the weak link in protecting

the information stored, processed, and transmitted by Government computers remains the people who manage, use, and operate them.

SEC. 3. ESTABLISHMENT OF COMPUTER SECURITY RESEARCH PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended by redesignating section 18 as section 19, and by inserting after section 17 the following new section:

"SEC. 18. (a) The National Bureau of Standards shall establish and conduct a computer security research program to address the problems of computer security in the Federal Government, with primary emphasis upon the prevention of computer-related fraud and abuse through the training of employees in computer security awareness and good security practice.

"(b) The program shall—

"(1) perform research and conduct studies to determine the nature and extent of computer security vulnerability in Federal agencies and their contractors;

"(2) devise administrative, management, and technical procedures and practices designed to protect the information stored, processed, and transmitted by Government computers; and

"(3) develop guidelines for use by Federal agencies in training their employees, and the employees of their contractors and of other organizations whose computers interface with Government computers, in computer security awareness and good security practice.".

SEC. 4. TRAINING BY FEDERAL AGENCIES IN COMPUTER SECURITY.

(a) In General.—Each Federal agency shall provide mandatory periodic training in computer security, under the guidelines developed pursuant to section 18(b)(3) of the Act of March 3, 1901 (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section, for all of its employees who are involved with the management, use, or operation of computers or other automated information systems and for all of the employees and other personnel of its contractors who are involved with the management, use, or operation of computers which interface with Government computers.

(b) Training Objectives.—Training under this section shall begin within 60 days after the issuance of the regulations described in subsection (c), and shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer and communications systems; and

(2) to encourage the use of improved computer security practices at Government facilities.

BEST COPY AVAILABLE

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing in detail the procedures and scope of the training to be provided by Federal agencies under subsection (a) and the manner in which such training is to be carried out.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

There are hereby authorized to be appropriated to the National Bureau of Standards for the fiscal year 1987, to carry out the computer security research program under section 18 of the Act of March 3, 1901 (as added by section 3 of this Act), such sums as may be necessary.

Mr. Brooks. Do you have an opening statement, Mr. Horton?

Mr. Horton. Yes, Mr. Chairman.

Mr. Brooks. Mr. Horton is our distinguished Member from upstate New York.

Mr. Horton. Thank you, Mr. Chairman.

I would like to join in welcoming our witnesses this morning, especially Congressman Glickman, the principal sponsor of this bill.

I want to commend you, too, Mr. Chairman, for convening this hearing and because, like you, I am one of the original cosponsors of H.R. 2889 and I feel it is an important piece of legislation and one that we should have these hearings on.

I am sure that within this committee as well as the Congress as a whole, there is agreement that steps must be taken to protect and better manage Government information. Each year the Federal Government is becoming more automated. We are the single largest buyer of automated data processing, telecommunications equipment.

The focus of this bill is protection and correct use of that equipment through the training of Government personnel who use these systems. The potential for losses and disruption to certain Government functions which would come from consistent illegal access is staggering. It is important that this legislation and the issue of computer security receive the attention that they urgently deserve.

I should add a caution that in this particular area, legislation and standards can only accomplish so much. With the exception of totally dedicated systems, it may be impossible to make totally secure our Government computer and telecommunications systems. Recent experiences have shown us that even those systems which appear to incorporate the most advanced security measures are sometimes subject to intrusion by ingenious hackers.

This does not mean, however, that we should sit idly by and let the situation continue. I think it is incumbent upon us to equip the Government's personnel with the best training and tools available to protect information and allow agencies to accomplish their missions.

I join with you in welcoming our witnesses. And I see by our schedule and who just walked in we will be having one of our former colleagues, Bud Brown, testify on behalf of the Commerce Department. He sat up here with me many years, and I look forward to having him testify for the first time before our committee.

Thank you, Mr. Chairman.

Mr. Brooks. Thank you, Mr. Horton.

Our first witness this morning is the Honorable Dan Glickman, a Representative in Congress from the State of Kansas. He is a principal sponsor of the Computer Security Research and Training Act of 1985 and has had a longstanding interest in this important matter.

Dan, I appreciate your taking the time this morning to give us the benefit of your views. Your prepared statement will be made a part of the record, and you may proceed as you see fit.

Welcome back to the committee.

STATEMENT OF HON. DAN GLICKMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF KANSAS

Mr. GLICKMAN. Thank you, Mr. Chairman and Mr. Horton. I am delighted to appear before this committee, especially with the work you have done on a whole variety of issues affecting Government operations and national security. And I am pleased that both of you are sponsors of this legislation to deal with computer security.

I don't have a prepared statement, so I will just pretty much talk briefly off the top of my head. But this committee is, no doubt, aware of a hearing record that the Science Subcommittee, that I had chaired in the past, made on a variety of computer security issues, and that information is fully available to this committee.

We have examined the issue of computer and communications security and privacy on two occasions. Back in the fall of 1983, we looked at the threat. We found that the most serious problems were with employees or others who have authorized access to computer systems and data; and while the hackers were an interesting part of that operation, the most serious problem in Government is with the insider, the person who has access.

We also found a lack of leadership from OMB and other central management agencies in assuring security of Federal systems and data.

In the fall of 1984, we also looked at it again, focusing specifically on the problems in the Federal Government. We found that the situation in the Government is a disaster waiting to happen.

Many Government systems are critical to the country, yet highly vulnerable to misuse, penetration or manipulation by disgruntled employees, terrorists, or others with criminal intent—the air traffic control system, law enforcement, banking systems, fund transfers, and privacy records on citizens.

We found again and again a lack of OMB leadership in this area. They did reissue a circular, A-71, but there has been in our judgment very little oversight of that dealing with computer security. And we found a need for greater awareness of users as to threats and vulnerabilities.

After this hearing, I think, the Government got together and asked what do we do. The response came not from beefing up the civil side of the picture; the response came from beefing up the defense, the national security side of the picture.

In June 1985, where you, Mr. Chairman, testified, we looked at NSDD 145, the National Security Decision Directive dealing with computer security, and we looked at questions regarding the process used in issuing this directive which we found was sorely lacking; and we felt there was much too much authority in the hands of the National Security Agency for establishing policy affecting civil agencies; and we found no voice in the security committee for privacy concerns; and we felt there were conflicts with existing law and Government directives for example, the Brooks Act.

Frankly, the major concern we had with this National Security Decision Directive was that it gave the defense and national security establishments authority over civil sector agencies in establishing policies on computer security. And we believe that is a serious problem and a serious mistake.

The problems are real. In my testimony—I don't want to go into a great deal—but looking at the HHS inspector general report, he talks about, in that report—which is available to your committee—a whole series of cases talking about the type of people who would be involved in security violations. Most were young. Most had some college, a broad section of jobs. Most crimes involved manipulating data in existing case files.

But one recommendation he makes, the IG of the HHS, is training for managers to make them better aware of vulnerabilities and internal controls so employees will know somebody is watching them.

This bill which I have sponsored, and which you have cosponsored with me, directs the NBS to conduct research and make periodic training available for employees. We believe the NBS is the proper home for this function as relates to the civil side of Government; since the National Security Decision Directive gives much too much authority to the NSA.

This bill further strengthens NBS's role in computer security and keeps a balance between civil and military interests. I think the threat to privacy is real as the Government turns to ever greater numbers of computers. The weak link is the people who use the computer. This bill will begin to address the people problem.

Again, I point out that my great concern about what the administration is proposing in the National Security Decision Directive is that they have no definition of "national security," and by implication and inference it looks to me like that directive gives the National Security Agency, and the Defense Department indirectly, complete authority over this problem as it affects the civil agencies.

I don't believe that is tolerable. I do believe they ought to have control over national security issues. Nobody is saying that they shouldn't. But issues affecting the computer security of the air traffic control system or banking records or Treasury Department records or HHS, or Social Security, or Veterans' Administration, should really not be within the purview of the NSA.

So, the purpose of this bill is to basically beef up the authority of the National Bureau of Standards to provide training in the civil side. And I appreciate the fact that this problem is receiving the level of attention it has in this committee, and I am hopeful that this committee will see fit to move this bill.

Thank you very much, Mr. Chairman.

Mr. **Brooks**. Thank you, Dan.

I have one question. Under the proposed bill, the National Bureau of Standards would pick up some additional responsibilities, as you know.

Mr. **Glickman**. Yes.

Mr. **Brooks**. Do you feel that the agency is ready and able to accept the expanded role?

Mr. **Glickman**. First of all, they have extensive capabilities in computer security. That is part of the work they have done for years.

Second, unofficially the agency is enthusiastic about this kind of work. It has the expertise and, I am told, it wants to take this particular work on. The only concern is that enough funds are forth-coming to do the work, and that is estimated to be about $1 million for the first year, $2 million or $3 million for the second, and $3 million to $5 million for the third year. That is a perennial problem we have in whatever program we have.

Mr. **Brooks**. As you know, of course, we have had serious problems with the OMB underfunding the NBS. OMB also—"by accident"—tries to cut their budget about $10 million every year. We all work on them—Mr. Fuqua works on them, you do, I do, Mr. Horton does—we all try. And NBS gradually gets enough money to continue their operations at their same level. However, OMB still seems reluctant to accept them as a viable and useful arm.

Mr. **Glickman**. I would say we just got to work on them harder. Once they accept the severity of the generic problem of computer security, we are going to have to put this problem into some institutional framework. And I say that the civilian side goes into the NBS, and the national security side goes with the NSA, or those type agencies, and they will just have to be funded.

Mr. **Brooks**. But the hackers will get them if they don't watch out.

Mr. **Glickman**. They are probably more worried about some of the hackers than they are about some of our other enemies. But they ought to be.

Mr. **Brooks**. Mr. Horton.

Mr. **Horton**. Thank you, Mr. Chairman.

Dan, we are happy to have you testify. I think it is an excellent bill, as I indicated. I am happy to be one of the cosponsors.

Why did you pick—or, why was the National Bureau of Standards picked to do this type of work?

Mr. **Glickman**. Primarily because of their previous work in computer-related issues. In their role in setting standards in the Government, they have developed a whole set of standards on utilization of computers. We felt that, given their role in standards, they would be in a good position to devise and develop security-related standards and devices and ranking those and rating those as they do in other areas of the Government.

They have an Institute of Computer Sciences and Technology that they have utilized in a generic sense, and it was a nonregulatory agency. Given all that, we felt it was the appropriate place to put it.

Mr. **Horton**. Do you have any idea how much time it would require to formulate a training program for Federal employees, and how much it might cost for implementation of the program?

Mr. **Glickman**. I would say the cost is, as I have said, $1 million for the first year, $2 million or $3 million for the second, and $3 million to $5 million for the third. That is based on estimates that they have given us. And my unofficial discussions with them indicate that they have the capability, inclination, and time to do it.

Mr. **Horton**. Thank you very much.

Mr. **Brooks**. Mr. Rowland, the gentleman from Connecticut.

Mr. **Rowland**. Thank you, Mr. Chairman.

Dan, I have just one question. With the research you have done and the hearings that you have conducted, do you sense that the security problem is one of a technical nature or a management nature?

Mr. **Glickman**. I would say it is both. Probably on balance it is more of a management-type problem and a human-type problem.

Now, obviously, there are some technology-related issues and problems here, in order to provide the protection so third parties don't come in and steal records on Social Security or veterans or steal Pentagon records. But the majority of it is human, management.

Mr. **Rowland**. Is it safe to say most of the program will be dedicated toward educating Federal employees on how not to be lax, how to be careful, how to protect the information?

Mr. **Glickman**. That is correct.

Let me give you one example. During our other hearings, we found that a Government agency was accessed using the same code that was used in the movie "War Games"—Joshua. And the code had not been changed. You know, it is simple things like changing the code every day that you would think would be done to protect this sensitive information. There are ways to protect against most incidents of that sort.

Then you need extraordinary technology to protect against extraordinary other types of incidents. But what we found is, there is just no concern on this. There is a concern for developing the software and developing the hardware, and most of that comes from manufacturers. But on the Government side, there just doesn't seem to be interest in protecting the information very well. So, that is one of the main reasons we want to move in this area.

You have a lot of people that have a lot of access to information. There have to be procedures to train them in how to use that information correctly

Mr. **Rowland**. Thank you very much.

Thank you, Mr. Chairman.

Mr. **Brooks**. Thank you, Mr. Rowland.

Mr. Glickman, I would ask you to join us if you have time. We would be pleased to have you sit with us.

Mr. **Glickman**. Mr. Chairman, unfortunately I have to chair a Judiciary subcommittee hearing on Superfund.

Mr. **Brooks**. Well, that is critical.

Mr. **Glickman**. To keep all the toxic waste from going to New York and south Texas.

Thank you, Mr. Chairman, Mr. Horton, Mr. Rowland.

Mr. **Brooks**. Thank you.

Our next witness is Milt Socolar, special assistant to the Comptroller General, U.S. General Accounting Office. Mr. Socolar is accompanied by William Franklin, Associate Director for Defense Management and Support Systems in the Information Management and Technology Division; and Gary Kepplinger, Acting Assistant General Counsel for Special Studies and Analysis in the Office of the General Counsel.

Milt, it is nice to see you again. Your prepared statement will be made part of the hearing record. Would you now please proceed.

STATEMENT OF MILTON J. SOCOLAR, SPECIAL ASSISTANT TO THE COMPTROLLER GENERAL, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY WILLIAM FRANKLIN, ASSOCIATE DIRECTOR, DEFENSE MANAGEMENT AND SUPPORT SYSTEMS, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, AND GARY KEPPLINGER, ACTING ASSISTANT GENERAL COUNSEL, SPECIAL STUDIES AND ANALYSIS, OFFICE OF THE GENERAL COUNSEL

Mr. SOCOLAR. Thank you very much, Mr. Chairman.

We are pleased to be here today to provide our views on H.R. 2889, entitled the Computer Security Research and Training Act of 1985. We, in the General Accounting Office, have long been interested in ensuring the security of automated information systems, and during the past decade have issued over 40 reports related to information system security.

As stated in the bill, information stored in Government computers and transmitted over connecting networks is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption. Studies of computer-related fraud and abuse in Government agencies show a costly and widespread problem of significant proportions.

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program to address problems of computer security in the Federal Government. There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage and transmission.

But in order to move ahead efficiently, we must have a clear understanding of the levels of security required for the range of information involved, and we must have established lines of responsibility and authority that are clear. Right now, there is considerable confusion on both of these counts.

Until recently, the Department of Defense developed computer and communication security standards primarily for national security information classified pursuant to Executive Order 12356. Unclassified information standards are provided by the National Bureau of Standards pursuant to the Brooks Act and provisions of Executive Order 11717.

The Office of Management and Budget and the General Services Administration also have major statutory responsibilities for computer and communication policy and standards—OMB pursuant to the Brooks Act, the Paperwork Reduction Act of 1980, and its general mandate for oversight of executive branch activities; while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No. 1.

In September 1984, the White House issued National Security Decision Directive 145, which establishes a Systems Security Steering Group as the focal point for both military and civilian information security. Together with an interagency committee, executive agent, and the national manager, the Steering Group is to establish and coordinate policies and review and approve budgets for computer and communications security efforts throughout the Government.

The directive provides for safeguarding from hostile exploitation systems that process or communicate sensitive information—and here the definition of sensitive information has been broadened to include any information affecting national security interests, whether classified or unclassified. NSDD 145 puts DOD and the civilian lead agencies in the same arena for large segments of information but without a clearly established division of responsibilities at least until the scope of the new definition of sensitive information is specified.

NSDD 145 does recognize that OMB, NBS, and GSA have major functions to carry out with regard to the security of information in automated systems, but the directive places ultimate control over the functions exercised by those agencies in the administrative structure it established. Activities of the civilian agencies are all made subject to NSDD 145 approval mechanisms.

The following provisions of H.R. 2889 overlap similar provisions of National Security Decision Directive 145. Section 3 of H.R. 2889 provides for NBS to: Engage in studies of vulnerability of information systems; devise procedures for the protection of such information; and develop guidelines for agency training programs.

NSDD 145 gives the Director of the National Security Agency, as National Manager, responsibilities to: Research and develop; examine Government telecommunications systems for vulnerability; and approve all standards for systems security.

These provisions would seem to provide for different agencies to perform similar functions. However, it is difficult to judge the precise extent of overlap that enactment of H.R. 2889 would engender since the full range of NSDD 145 and its overall applicability to civilian agencies is unclear.

While we support the need for a comprehensive computer security research and training program as proposed by H.R. 2889, we would suggest that since computer security research and training programs are carried out by DOD for all Federal agencies for both classified and much unclassified information, that a clear understanding of DOD's role versus the roles of OMB, GSA, and NBS be established in conjunction with consideration of H.R. 2889.

In this connection, it should be noted that there is a potential that we will commit ourselves to the development and teaching of inordinately expensive approaches to computer security. DOD, in its approach to security, seeks to counter identified or perceived threats to the national defense, treating costs as a decidedly secondary factor in determining the degree of protection required.

The National Bureau of Standards, on the other hand, emphasizes a risk management approach that uses costs as a primary determinant. Now that NSDD 145 has created a category of information designated as sensitive unclassified information, there is a potential, if not a likelihood, with DOD taking the lead, for excessive expenditures to protect unclassified information.

More importantly, the broad leadership role that NSDD 145 assigns predominantly to DOD raises basic questions concerning the extent to which the Defense Establishment should be involved in policy formulation and program administration within the Government's civilian agencies. There can be no question that there is unclassified information stored in Government computers and transmitted through communication systems, the unauthorized disclosure or disruption of which could affect our national interests.

It does not follow that DOD must be responsible for deciding what should be done to protect this information. The assignment of that responsibility is an issue of long-range importance that should be thoroughly considered by the Congress.

That completes my prepared statement, Mr. Chairman. We would be pleased to answer any questions you or any other members of the subcommittee may have.

[Mr. Socolar's prepared statement follows:]

STATEMENT OF
MILTON J. SOCOLAR
SPECIAL ASSISTANT TO THE COMPTROLLER GENERAL
UNITED STATES GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to provide our views on H.R. 2889 entitled the "Computer Security Research and Training Act of 1985." We have long been interested in ensuring the security of automated information systems and during the past decade have issued over 40 reports related to information system security. As stated in the bill, information stored in government computers and transmitted over connecting networks is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption. Studies of computer-related fraud and abuse in government agencies show a costly and widespread problem of significant proportions.

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program to address problems of computer security in the federal government. There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage and transmission. But in order to move ahead efficiently we must have a clear understanding of the levels of security required for the range of information involved, and we must have established lines of responsibility and authority that are clear. Right now there is considerable confusion on both of these counts.

Until recently the Department of Defense developed computer and communication security standards primarily for national security information classified pursuant to Executive Order 12356. Unclassified information standards are provided by the National Bureau of Standards (NBS) pursuant to the Brooks Act and provisions of Executive Order 11717. The Office of Management and Budget (OMB) and the General Services Administration (GSA) also have major statutory responsibilities for computer and communication policy and standards--OMB pursuant to the Brooks Act, the Paperwork Reduction Act of 1980, and its general mandate for oversight of executive branch activities, while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No.1.

In September 1984, the White House issued National Security Decision Directive 145, which establishes a Systems Security Steering Group as the focal point for both military and civilian information security. Together with an inter-agency committee, Executive Agent, and the National Manager the Steering Group is to establish and coordinate policies and review and approve budgets for computer and communications security efforts throughout the government. The directive provides for safeguarding from hostile exploitation systems that process or communicate sensitive information...and here the definition of sensitive information has been broadened to include any information affecting national security interests whether classified or unclassified. NSDD 145 puts DOD and the civilian lead agencies in the same arena for large segments of information, but without a clearly established division of responsibilities at least until the scope of the new definition of sensitive information is specified. NSDD 145 does recognize that OMB, NBS, and GSA have major functions to carry out with regard to the security of information in automated systems, but the directive places ultimate control over the functions exercised by those agencies in the administrative structure it established. Activities of the civilian agencies are all made subject to NSDD 145 approval mechanisms.

The following provisions of H.R. 2889 overlap similar provisions of National Security Decision Directive 145. Section 3 of H.R. 2889 provides for NBS to

--perform research and conduct studies to determine the nature and extent of computer security vulnerability in federal agencies and their contractors;

--devise administrative, management, and technical procedures and practices designed to protect the information stored, processed, and transmitted by government computers; and

--develop guidelines for use by federal agencies in training their employees, and the employees of their contractors and of other organizations whose computers interface with government computers, in computer security awareness and good security practice.

NSDD 145 gives the Director, National Security Agency, as National Manager, responsibilities to

--conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information;

--examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including these involving monitoring of official telecommunications, shall be conducted in strict compliance with law, executive orders and applicable presidential directives. No monitoring shall be performed without advising the heads of the agencies, departments or services concerned; and

--review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

These provisions would seem to provide for different agencies to perform similar functions. However, it is difficult to judge the precise extent of overlap that enactment of H.R. 2889 would engender since the full range of NSDD 145 and its overall applicability to civilian agencies is unclear.

While we support the need for a comprehensive computer security research and training program as proposed by H.R. 2889, we would suggest, that since computer security research and training programs are carried out by DOD for all federal agencies for both classified and much unclassified information, that a clear understanding of DOD's role versus the roles of OMB, GSA, and NBS be established in conjunction with consideration of H.R. 2889.

In this connection, it should be noted that there is a potential that we will commit ourselves to the development and teaching of inordinately expensive approaches to computer security. DOD, in its approach to security, seeks to counter identified or perceived threats to the national defense, treating costs as a decidedly secondary factor in determining the degree of protection required. The National Bureau of Standards, on the other hand, emphasizes a risk management approach that uses costs as a primary determinant. Now that NSDD 145 has created a category of information designated as sensitive unclassified information there is a potential, if not a likelihood, with DOD taking the lead, for excessive expenditures to protect unclassified information.

More importantly, the broad leadership role that NSDD 145 assigns predominantly to DOD raises basic questions concerning the extent to which the defense establishment should be involved in policy formulation and program administration within the government's civilian agencies. There can be no question that there is unclassified information stored in government computers and transmitted through communication systems, the unauthorized disclosure or disruption of which could affect our national interests. It does not follow that DOD must be responsible for deciding what should be done to protect this information. The assignment of that responsibility is an issue of long-range importance that should be thoroughly considered by the Congress.

- - - - -

That completes my prepared statement, Mr. Chairman. We would be pleased to answer any questions.

Mr. **Brooks**. Thank you very much, Mr. Socolar.

Is the lack of clear enforcement authority going to hamper the effectiveness of the NBS to manage the program?

Mr. **Socolar**. The agency compliance with security standards has been spotty, and I think that has been very generally recognized. And the National Bureau of Standards, in fact, has no enforcement mechanism in place.

But the issue really is one of enforcement, and whether it is located in NBS or elsewhere is not the primary question. The fact of the matter is that OMB today has enforcement authority over standards in the Paperwork Reduction Act. And the basic issue, again, lies in the extent or the lack of extent to which enforcement procedures have been implemented throughout the Government.

Mr. **Brooks**. Now, Milt, under the Brooks Act, GSA is assigned certain authorities. Wouldn't GSA be a logical place to implement the recommendations of the NBS and its guidelines in computer security? Would't then the companies be more aware of the necessity of building in security when they sell computers to the Government—at least minimum security precautions?

Mr. **Socolar**. That certainly would be a logical place under the regulations that GSA issues. Under the procedures, it provides for even a waiver of those regulations in extraordinary circumstances. But they do have the authority right now under the Brooks Act to govern the procurement of computers and software.

Mr. **Brooks**. Right.

What are the problems associated with using a classification category such as "unclassified information with a national security interest?"

Mr. **Socolar**. That, to me, is one of the really basic issues, Mr. Chairman, that underlies the whole problem that we are discussing. On the one hand, if the definition of "information that has security implications for the national interest" is drawn too broadly, we would have the DOD and the apparatus set up under 145 controlling an enormous amount of information in our society.

On the other hand, if it is drawn too narrowly, we have the issue of large amounts of sensitive information that are indeed important, which need attention, that is not being provided under the current administration.

Determining the appropriate mechanism for addressing this information involves tradeoffs among economic, political, social implications such as the impact of security measures on the agency's ability to freely exchange information in support of their missions.

If resolution of this issue favors expanding the scope to cover the full range of critical systems, then the administration must be sensitive to these political considerations.

Mr. **Brooks**. Milt, do you believe the Bureau of Standards has sufficient support from the Commerce Department and OMB to successfully fulfill the additional responsibilities assigned under the proposed bill?

Mr. **Socolar**. I can only judge the extent of support they have by the amount of attention that is being paid to the problem. And, based on the work we have done, I would have to conclude that it has been very spotty and that it doesn't appear that the appropriate support—whether from Commerce or OMB—is being provided.

Mr. Brooks. All right. What role can the National Security Agency play in assisting the National Bureau of Standards' computer security program as envisioned under the bill?

Mr. Socolar. The National Security Agency does have expertise in this area and could very well provide good technical support to the National Bureau of Standards.

Mr. Brooks. Mr. Horton.

Mr. Horton. Thank you, Mr. Chairman.

Milt, we are glad to have you back with us again with your colleagues.

You seem to indicate, on page 5, that it might be more costly for DOD to set computer security standards than the NBS. What do you base that conclusion on?

Mr. Socolar. That is not a conclusion as much as it is an expectation based on the approach that the Department of Defense takes to any issue relating to security. The Department of Defense considers that if a determination is made that information is important to the national security, it then moves toward setting levels of security to protect that information without regard to cost as a primary determinant or a determinant that would affect the level of security provided.

The NBS, on the other hand, approaches the issue of security in these systems with a consideration of the cost-benefit ratio involved and the manner in which that security can be managed to effectuate the security in the final analysis.

Mr. Horton. I guess what you would have to determine, really, is what the purpose is of the security from the standpoint of the national security in the Department of Defense, and that is one purpose and one aspect.

I would imagine that that would be a lot more thorough than what the National Bureau of Standards might set down as the goal for the security check.

Could you comment on that?

Mr. Socolar. Yes. I think that is absolutely correct.

The issue really lies in the kind of definition we are going to get for information that is sensitive and is security-related.

Mr. Horton. Is there a need for the DOD to look at all of the computer systems in the Federal Government for national security purposes?

Mr. Socolar. I think there is a need for the Department of Defense to look at the kinds of information that are stored in Government computers and transmitted in Government operations. I think that it is in the definition of that information that we are going to have the kinds of problems I am referring to.

Mr. Horton. But how do we get out of this box? I can see on the part of the Defense Department if they have the goal of making secure all computers as far as national security goes, in their own computers, that would be one thing. But you heard the testimony of Congressman Glickman.

When they are talking about other agencies, civilian agencies, as it were—say, the Department of Interior or Commerce or whatever it might be—is national security involved in those computer systems so that you have to have the same type that they have—they have to have the same type of security that the DOD would level?

Mr. **Socolar**. I am not sure that I am able to specify precisely what kind of information should be considered as national security information. But in light of what we are talking about in terms of the broad reach of 145, that is the very issue that I think needs to be debated in the Congress rather than summarily——

Mr. **Horton**. I understand that.

In other words, what you are saying is that 145 in essence has given this broad stroke to the DOD to look for national security issues, as it were. But I am trying to get your input as to what the GAO thinks is necessary with regard to division of it.

I can see the NBS would have a different security goal than the DOD would have. I can see also—this starts from the question that I asked—as to how much it would cost to do the job. The National Bureau of Standards would have a much less high standard for security. Probably all they would be looking at is the type of thing that we try to protect from the Freedom of Information Act.

Mr. **Socolar**. The basic test, it would seem to me, would be that the Department of Defense take cognizance over that information which is classified; and any information which, after examination, remains unclassified should remain with the civilian agencies.

Mr. **Horton**. Thank you very much.

Mr. **Brooks**. Mr. Rowland, the gentleman from Connecticut.

Mr. **Rowland**. Thank you, Mr. Chairman.

Mr. Socolar, are you aware of any infringements the DOD may have already made under the authority of any other agency while acting under 145?

Mr. **Socolar**. No, I am not aware of any specific infringements. I am aware, though—and I think we all are—of the policy statement that has been issued attempting to define the reach of 145 on the issue of what is sensitive information with security implications, and that policy draft is a very, very broad definition which, if not narrowed, gets us precisely into the arena we have been talking about.

Mr. **Rowland**. But you don't see it as an infringement at this point?

Mr. **Socolar**. I am not aware of any at this point.

Mr. **Rowland**. Thank you, Mr. Chairman. That is all I have.

Mr. **Brooks**. Thank you very much.

Thank you, gentlemen, for being here—Mr. Franklin, Mr. Kepplinger. We appreciate your contribution to the hearing.

Our next witness is the Deputy Secretary of Commerce, Clarence J., better known as "Bud," Brown.

We are glad to have you back. We remember his daddy.

Now, Clarence's nickname is "Bud," which is fairly friendly and innocuous. His daddy's nickname was "The Old Bear," which was not quite as innocuous but he was equally intelligent and equally gracious.

Bud, we are glad to have an alumnus of the committee appear before us. We are appreciative of your sharing the Department's views on this important matter. You may proceed as you see fit.

Who do you have with you?

STATEMENT OF CLARENCE J. BROWN, DEPUTY SECRETARY, U.S. DEPARTMENT OF COMMERCE, ACCOMPANIED BY RAYMOND G. KAMMER, JR., DEPUTY DIRECTOR, NATIONAL BUREAU OF STANDARDS

Mr. BROWN. I will cover that, if I may, Mr. Chairman.

Mr. BROOKS. All right. I won't introduce him, then.

Mr. BROWN. Mr. Chairman and members of the committee, I want to thank you for the opportunity to testify on the important subject of computer security. I am accompanied by Ray Kammer, Deputy Director of the National Bureau of Standards.

My testimony today will center on the computer security program being carried out within the Department of Commerce at the National Bureau of Standards; on H.R. 2889, presently being considered; on the National Security Decision Directive 145; and on a proposed Governmentwide program in computer security.

Public Law 89-306—authored by you, Mr. Chairman—established the roles of several organizations for improving the utilization of computers within the Federal Government. The Department of Commerce delegated its role of developing Federal information processing standards for improving the effective use of computers to the National Bureau of Standards. The President later delegated his authority to issue the Federal information processing standards to the Secretary of Commerce.

The Institute for Computer Sciences and Technology [ICST] was established within NBS to carry out this legislative mission. The Institute established a computer security program in fiscal year 1973. The testimony of Mr. Burrows, Director of this Institute, outlines the achievements of this program, and he can address its technical aspects.

With world trade increasing and American industries buying, selling, developing technology, manufacturing worldwide and financing worldwide, we also see that the distinction between computers and communications is becoming blurred; in effect, it is developing into a single industry.

New technology in general use for transfer of data involves computers, satellites, over-the-air broadcasting, land lines, and other data transfer media that must be considered to achieve a secure system for both public agencies and private users.

Security is important not only for national security applications but also to private companies that transfer data and funds worldwide by satellite. The private sector wants to be able to assure security of its private data from other companies, other countries, and in fact also from the U.S. Government.

The early role of NSA and its current role under NSDD 145 is to address communication and computer security needs including even description for national security purposes.

The current NBS security program emphasizes the development of technical and administrative methods for protecting the integrity, confidentiality and availability of computer data in both the public and private arenas. NBS now relies on the research and development efforts of other Government entities, primarily the Department of Defense, for some of its work. The breadth of the NBS computer security program and utility of the resulting standards

BEST COPY AVAILABLE

and guidelines has been widely recognized. The technical depth of the research program of the DOD promises significant results in specialized technical areas. Appropriate technology has been transferred from the research program of the Department of Defense to the NBS, but there has existed no independent research activity of sufficient scope to support the security programs sought by many non-DOD organizations and activities.

The Department of Commerce endorses the intent of the bill, but believes our existing statutory authority under the original Brooks Act and ongoing activities preclude the need for additional legislation.

I would now like to present our views on NSDD 145. The directive states a set of requirements for protecting classified national security information and other sensitive information concerning the vital interests of the U.S. Government. It then establishes an administrative mechanism for achieving the goals of this protection program.

The directive specifically states, and I now quote: "Nothing in this directive amends or contravenes the provisions of existing law, Executive orders, or Presidential directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse and waste." As this has been the thrust of the computer security program at the National Bureau of Standards, we see no change, other than a requirement for coordination, due to the directive. We feel that the existing legislation and the directive are consistent.

Finally, we believe that a joint research program in computer security is workable and desirable. The Department of Defense would focus on national security, and the Department of Commerce on civil concerns, with some cross-referencing between the two. The efforts would be coordinated for program effectiveness and to avoid duplication.

Mr. Chairman, thank you for the opportunity to testify, and I am available to answer any questions you may have, or other members of the committee.

Mr. BROOKS. Mr. Secretary, I want to thank you for being here. I have a couple questions that you might be able to handle without much trouble.

Does the Department fully support the ADP standards program under Public Law 89-306?

Mr. BROWN. We do, indeed. And we would differ with the testimony of the previous witness to the effect that there has been any lack of interest or support in the program.

As a matter of fact, we have recently established a cross-cutting organization within the Commerce Department that would address precisely the issues on which I have testified between NBS, the National Telecommunications and Information Agency, which handles the international communications aspects of both the Federal Government and our interest in the use of those international communications methods for the private sector, and with the other agencies in the Department that deal with international trade problems, because we are transferring both publicly and privately some very significant data and information.

As a matter of fact, Mr. Chairman, as I testify now before you there is a press conference, I guess you would call it, going on at the Defense Department about a study done on Soviet acquisition of militarily significant Western technology—an update, it is called. That particular study talks about the methods by which the Soviet Union—and therefore, presumably other countries in the international scheme—are looking at not only defense data and things related to military security, but also technical data of private companies for what that infers about their technological needs in their society.

So, it is both in the public and private sector that these issues are important since we deal with the trade matters in the Department of Commerce. Then we think that the ICST's work and the work of MTIA and the work of the Trade Administration are very important and ought to be interrelated.

Mr. **Brooks**. Mr. Secretary, the Institute's budget has been decreased or frozen over the last 5 years.

If its budget for 1987 would be cut again, what would be the impact on the Institute's current responsibilities, some of which you just delineated, as well as the new ones envisioned under the proposed bill?

Mr. **Brown**. As you know in preparation of budgets, which is one of my responsibilities at the Commerce Department, the Commerce Department and other Federal Government agencies attempt to first address the interests of the administration in trying to reduce the Federal deficit, now $200 billion, and a concern for both the Congress and for the administration.

As such, the position of the Office of Management and Budget, the administration, and the Commerce Department has been that certain functions within the ICST might be subject to private undertaking or private financial support. Many of the activities of the National Bureau of Standards are, in fact, supplemented in their financing by private sector participation in the activities of NBS, and some of them are complemented by private activities in a similar vein, that is similar research efforts, and so forth, and then the information is exchanged.

So, with reference to the preparation of the ICST budget the administration has held in the past that the budget ought to be supplemented by private sector support in view of the fact that we are doing some work that might also be done by the private sector.

Mr. **Brooks**. I would like to observe that one of your predecessors—a very able man who has gone on to other responsibilities now in the OMB—Joseph R. Wright was Deputy Secretary of Commerce on October 21, 1981, when he made these comments about the Brooks Act and the National Bureau of Standards. Mr. Wright said that the issuance of 50 Federal information processing standards and 35 guidelines will save the Federal Government $120 million in new procurement costs each year. This indicates to me that the National Bureau of Standards, if funded adequately and appropriately supported, will save the Government millions and millions of dollars more than we will ever spend on it.

I would hope that you take a look at this and that we could get a little closer coordination as we try to work on the deficit. We might save a lot more on the deficit by bolstering the Bureau of Standards.

Mr. **Brown**. Mr. Chairman, understand the 2 years that have been in the process of preparing budgets the National Bureau of Standards budget has been increased over the mark given us by OMB, Office of Management and Budget, in its general and broad functions, not specifically in ICST, but in other areas.

As we try to address the unique technology that are developing in such things as ceramics, biotechnology, and so forth, some of the existing programs in order to achieve that budget balance have been recommended for curtailment. The Congress has, in effect, responsored some of those older programs and has, in effect, in this way reduced some of the new cutting edge technology programs we have proposed. So I would agree with you, unfortunately—I don't always agree with the Congress—and what they did in the budget for 1986, for instance.

Mr. **Brooks**. Mr. Horton.

Mr. **Horton**. Thank you, Mr. Chairman.

Bud, we welcome you here, and as far as I know this is the first time you have testified before the committee and we are happy to have you.

Mr. **Brown**. As a matter of fact, Mr. Horton, it is the first time for me to testify before any congressional committee. I am surprised it took so long for me to use my appearance opportunity.

Mr. **Brooks**. I must say I think he has done very well. He was a member of this committee for many years.

Mr. **Horton**. Yes; he did very well, I agree.

Mr. **Brooks**. Mr. Brown had effective terminology characteristics as a Member, but as Deputy Secretary—he is acting as Secretary now because Secretary Baldrige is out of town working somewhere; I hope he is riding a horse in a roping contest and enjoying life——

Mr. **Brown**. Down in Texas.

Mr. **Brooks** [continuing]. He has done well. His statement was concise, not overpartisan. You know he has a tendency to do that. I thought it was a good statement. He isn't too keen on the legislation, and you have to read it carefully. He says existing statutes and regulations would preclude absolute necessity of anything else. You all understand that. It is a nice way—I thought it was a gracious way to say he isn't for the bill at all. Anyhow, we are glad to have you here.

Mr. **Brown**. Mr. Chairman, if I may, what I said was that you covered this issue so effectively in your initial legislation that was passed in the 89th Congress, that we don't think that there is a need for additional legislative authority. We think you have covered it then, and we would be happy to undertake what, may I say, the pejorative legislation you have proposed, attempts to accomplish. We see no need for additional authority.

We think that authority exists already thanks to the prescience of the chairman.

Mr. **Brooks**. I keep trying to do better though, I don't rest on what we did 15 or 20 years ago; we keep trying to do better.

Mr. **Horton**. Bud, you said it well—and one thing he did have, Mr. Chairman, when he was on the committee, he was tenacious and he still is.

Mr. **Brooks.** He was tenacious. In question after question, he interrogated Bud Grant for an hour and a half.

Mr. **Horton.** The only question I wanted to ask, if for some reason you didn't have the Institute, private industry would probably set the standards—what ramification would this have for the Goverment agencies?

Mr. **Brown.** Now, we have two questions, Mr, Chairman, and I am not sure I understand, Mr. Horton.

Mr. **Horton.** You were talking earlier about the budget problem.

Mr. **Brown.** Yes.

Mr. **Horton.** And you feel, you felt there was adequate funding, and so forth.

But if for some reason there was not adequate funding or there was no Institute for some reason, the ICST, then probably the private industry would tend to move in to set the standards or would be asked to. You did indicate that you thought that they ought to be participating.

And you say they are participating. That was what the administration was desiring that the private sector be involved in setting standards.

What ramifications would this have for Government agencies?

Mr. **Brown.** Well, if I may, on the question of setting standards, that is the function of the Government in terms of identifying for all companies, competitive markets, same industry markets, or even different industries, certain standards.

We have been setting standards since we developed the platinum inch back around 1900.

With reference to whether there are common plug-in characteristics within the industry, that is frequently an industry decision. The standards for all industries may be the same but the kind of equipment that they develop may be different.

If I may just for a minute, first, the trade aspects of this are significant. You may recall almost 40 years ago now, the Federal Government made a decision about the way color television would be developed.

As I recall, RCA had a system that was electronic, CBS had a system that was wiring disks, and a Federal agency made a decision that the most promising for future development was the RCA electronic system, and that became the technological direction in which the industry went off to improve color television.

At NBS we try to set standards, but we don't determine what the common approach of an industry would be necessarily in any particular area.

Now, industry does its own research. We do research to help set the standards, but industry does its research on establishing products and developing the science and technology of it.

We think those two things can work together, but that when it comes to setting a single standard for all computers as to what they ought to be, the industry has resisted that because they think that new technological developments help keep American computers ahead of their foreign competitors.

On the other hand, there are certain market aspects that the Japanese sometimes undertake, and say:

OK, we stop development now, everbody makes the same kind of a product, and we try to take the world market with a lower price because the common production of those products at a lower price is what is going to drive the market.

The computer industry in this country has not done that, nor have we encouraged them to do it. We raise the question every once in a while about what further we can do to help them come to common conclusions and plug-ins that make all computers work together, and, as a matter fact, the NBS has done work in getting computers to talk to each other to help operate machinery that is different and operate on different computers, but there is a need for the coordination of that machinery.

So, we do some of that. None of that gets into the security question, but it deals with our role in setting standards.

Mr. HORTON. Well, thank you very much.

Mr. BROOKS. Thank you, Mr. Horton.

Mr. Rowland, the gentleman from Connecticut—he has already gone.

I want to tell you, Mr. Secretary, we appreciate your being here, and also Mr. Kammer. Thank you.

Mr. BROWN. I hope it is helpful, Mr. Chairman, and I hope if you have any technical questions that the next witness can address those technical questions on the terms of how we are dealing in the security area. And we do feel, Mr. Chairman, to reiterate my position, and the position of the Department, that while there is—I want to agree with Mr. Socolar's testimony to some degree, there are cross-cutting responsibilities here, but we think we have the authority, and we already produce the training material for people to use computers in a secure way.

The other agencies of Government can require training if they wish. The administration could require that by order if they wished, and we have produced the methods by which those security processes and security methods can be applied to Government computers, and we help the private industry now in establishing their security programs for their computers.

Mr. BROOKS. Thank you very much, Mr. Secretary.

Our next witness is Jim Burrows, Director of the Institute for Computer Sciences and Technology at the National Bureau of Standards. I want to welcome him back to the committee. He has been one of the people who should get a big share of the credit for his enforcement and support of the Brooks Act over the years. The GSA has said it saved the Government about $6 billion, and Mr. Burrows' strong support at a technical level has helped to make that possible.

We are delighted to have you here.

Your statement will be made a part of the record and we will hear whatever you have to say.

STATEMENT OF JAMES H. BURROWS, DIRECTOR, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY, NATIONAL BUREAU OF STANDARDS

Mr. BURROWS. Thank you, Mr. Chairman.

Mr. Chairman, and Mr. Horton, I thank you for inviting me to speak to you today and for your interest in this critically important subject. I ask permission to summarize my statement which I would like to submit for the record.

Mr. BROOKS. Without objection, the gentleman can proceed.

Mr. BURROWS. The need for computer security has never been greater than it is today. The legislation that you are considering, H.R. 2889, takes note of the factors that contribute to this pressing need, the Government's dependence on computers, the scale of Government computer operations, the widespread dispersal of personal computers throughout the Government, and the valuable and sensitive information that is contained in Government computer systems.

Rapidly changing technology and the escalating use of computers will continue to make computer security a high priority issue in the future. We see that it is impossible to return to manual methods once an organization adopts automated data processing methods.

To achieve efficient information interchange, we must strive for standard, interoperable hardware and software systems. At the same time, however, widespread use will increase the vulnerability of our systems to external and internal threats.

To prevent serious accidents and intentional activities that cripple our ability to carry out data processing operations and to avoid compromise of sensitive information, we must stimulate an awareness for the need for computer security in managers and users of computer systems.

This is the key element in a campaign to improve computer security, and this is the thrust of H.R. 2889. I believe that this legislation addresses clearly established needs for computer security research and for training the people who manage, use, and operate Federal Government computers.

Training for computer security is going to be essential in tomorrow's computing environment. The reports about the high level of personal computer use in Federal agencies highlight the urgency of this need. Issuing directives to improve security will not be enough. Structured, organized, systematic training opportunities will be a must if the Federal Government expects to exploit the use of advanced technology for improved staff productivity and reduced costs of Government.

The legislation calls for the National Bureau of Standards, NBS, to conduct computer security research leading to the development of technical procedures, practices, standards, and guidelines for use in training. Many guides and reports that NBS has developed are already available and widely used in training programs.

However, in order to deal with the urgency of the computer security problem as laid out in H.R. 2889, it will be necessary for NBS to expand greatly the kinds of materials it develops and to develop materials suitable for widely different needs and not just training.

Computer security awareness programs must be available not only for the managers and users of automated information systems, but also for other agency personnel such as internal auditors, inspectors general personnel, and budget analysts and managers. This will be essential to enable corrective actions to be proposed and implemented for information system development, operation, and modification.

These awareness programs and the renewed emphasis on computer security will also heighten the demand for timely products from NBS. Further, as new uses are made of computers and as new users become familiar with computer capabilities, new weaknesses will be exposed. Therefore, continuing attention to research and the development of effective protective methods will be needed.

The Institute for Computer Sciences and Technology at the National Bureau of Standards is currently carrying out a program of research in computer security areas. This program was started in 1972 as a component of our responsibilities under Public Law 89-306, the pioneering legislation authored by Chairman Brooks to improve the efficient and effective use of computers in the Federal Government.

Responsibility for developing computer security standards and guidelines is also specifically assigned to the Department of Commerce under OMB circulars, and has been delegated to NBS. The Paperwork Reduction Act also provides additional legislative authority to carry out our program.

The problems that we are addressing are broad in scope and include many different hazards—for example, physical damage to computers, accidents, destruction of data, theft of data and software, programming and data errors, omissions, and abuse of computing resources.

While breaking into systems and computer crime are serious incidents, they are just one aspect of the problem. We are also concerned about the losses that result from processing incorrect data, from interruptions to data processing, and from lack of controls to prevent misuse of computers by authorized personnel. A vast amount of unclassified, but sensitive, information must be protected. This includes personal, proprietary, and other information protected under the Privacy and Freedom of Information Acts.

ICST's program is targeted to three principal objectives: Computer integrity—this means the ability to prevent or detect unauthorized modification or destruction of computer information; confidentiality, the ability to prevent unauthorized disclosure of information; and availability, the ability to assure that processing resources are ready and waiting when needed.

Failure to achieve these objectives in Federal Government computing operations could result in undesirable events ranging from threats to national security to denial of benefits to citizens, loss of Government money and resources, human injury, or loss of life.

Under our legislative charter and policy directives, we develop management guides, test methods, performance measures, technical information and advice, guidelines, and standards.

In developing our products and services we pay particular attention to the problems of Federal computer users and to the development of cost-effective security methods that are appropriate to the information and systems to be protected.

We also emphasize good preventive techniques because it is often more cost effective to avoid costly errors and accidents than to recoup after an expensive mistake. We have found that State and local governments, business, and industry users have problems similar to the Federal Government's and that our technical products are used by the private sector as well as by the public sector.

They are frequently used as the basis for training and education programs such as those conducted by the Small Business Administration and the Office of Personnel Management.

In the area of computer security and risk management, as well as in other program areas, we work closely with users in large and small organizations to learn about their experiences and their needs for technical and management solutions to their computer utilization problems.

Because we are a small organization, we believe that the best way to achieve change is to work through other organizations. We sponsor, and participate in, conferences, workshops, and meetings to share information and to keep users and industry informed of our activities, as well as to learn what others are doing.

We respond to requests for advice and consultation, we participate in training seminars to the extent that we can, and we provide direct technical assistance to Federal agencies on a reimbursable basis for a limited number of projects that are related to our program.

I especially want to emphasize our work with the National Security Agency [NSA] and the National Computer Security Center [NCSC]. NSA has conducted extensive research in the development of security technology for national defense applications.

We are continually evaluating the applicability of these research activities to the civilian side of Government and the private sector, so that we can transfer appropriate technology to the users who need it. Guest workers from NSA are working with ICST staff, and we maintain close staff contact on technical issues. We will be hosting the eighth national conference on computer security with DOD later this month. The conferences have been well attended by both Government and industry participants.

We have cooperated with the General Accounting Office in their reviews and evaluation of agency computer security and have provided briefings and seminars on computer security to many Federal and State government organizations.

We also participate in meetings sponsored by business and industry organizations to learn what they are doing and to make their good practices available to Government users. Groups that we work with include EDP auditors, computer security professionals, internal auditors, universities, bankers, lawyers, and computer user groups.

As a result of our interactions with these groups, we are in a position to analyze user experiences and to identify best practices based on currently available technology.

We have published a variety of reports, documents, guides, and studies conveying what we have learned. Through our contacts at many levels and with many organizations, we try to leverage our products so they reach a wide audience. For example, we are a clearinghouse of information that we have collected on computer security training opportunities, reading lists, and computer security services. This information is available electronically on a computer-based bulletin board.

We cooperate with business and industry to develop national and international consensus standards for computers and networks. We can do this effectively because of our knowledge of user and industry needs for standards and the position of trust that we have as objective participants in the standards process.

Our goal is to stimulate the development of off-the-shelf commercial products that will expand choices, provide for interoperability of components and systems, and broaden opportunities for applications of new technology.

We are working with voluntary standards development groups sponsored by the American National Standards Institute, Institute of Electrical and Electronics Engineers, the International Organization for Standardization, the American Bankers Association, and other national and international groups. We also participate with the National Communications System and the General Services Administration to develop Federal standards for telecommunications.

Another important collaborative effort is our work with the Department of the Treasury to develop a policy to assure the integrity of electronic fund transfers.

Last year Treasury issued a directive requiring the use of a voluntary standard for Financial Institution Message Authentication, to protect the billions of dollars that are transferred electronically every day. ICST was a major contributor to the standard, and to other voluntary standards developed for the private sector banking community.

The Treasury directive requires that all of its bureaus' EFT transactions be authenticated using data encryption techniques. Authentication is a process of coding and decoding significant phrases in a message to assure that it has been sent by an authorized party and has not been tampered with during transmission.

ICST staff has been working with the voluntary standards community to draft a standard for protecting the secret keys that are used in coding and decoding messages.

Automated key management techniques that were developed and patented by ICST staff are specified in this standard. Available on a license-free basis to organizations that want to use them, these techniques are being implemented in ICST's laboratory to help organizations test their products for compliance with the standard. A list of certified message authentication devices and techniques will be developed by Treasury with ICST and National Security Agency assistance.

ICST is working in conjunction with the National Security Agency in developing proposed standards for data integrity and security in distributed computer networks. These efforts will focus on methods of securing data communications using data encryption techniques in a network of microcomputers.

Commercially available software, protocols, and equipment will be used whenever possible. The network and primary security features will be unclassified, but will be designed to support more stringent security requirements for special applications.

Security of personal computers is currently under investigation. We recently issued a guide explaining security threats in the use of small computers and ways to reduce the risks. We are looking at a wide range of commercially available computer security devices for small systems to develop guidance for users in selecting cost-effective security equipment.

We are participating in a joint project with the President's Council on Integrity and Efficiency to develop criteria for auditors to use in establishing their work plans for auditing for security and controls throughout the life cycle of an automated information system. Specific guides and recommendations will be issued through this effort.

Security must be an integral part of overall systems planning. Therefore, we must be concerned about security in all of our technical activities, and we must address all aspects of computer system development and operations. This includes software systems, networks, storage media, and other hardware components. The weak link can appear anywhere in a complex system, and a comprehensive approach is needed to assure that strengths in one part of the system are not wiped out by weaknesses elsewhere.

As you know, the Department of Commerce is one of the members of the National Telecommunications and Information Systems Security Committee established under National Security Decision Directive 145, and we have been participating in the Subcommittee on Automated Information Systems Security.

A major focus is the development of definitions of sensitive, but unclassified, Government or Government-derived information which has an impact on national security.

We believe that we can contribute to the implementation of NSDD 145 which complements, but does not substitute for, our work. We expect to continue to issue Federal information processing standards for automated information processing security under our current authorities.

Those that are appropriate for issuance under NSDD 145 will be submitted for processing under the procedures that are being developed by the National Telecommunications and Information Security Committee.

For example, Federal Information Processing Standard 112, password usage, is the first approved FIPS that will also be processed under the directive. Its intended use includes protecting passwords in both the classified and unclassified information environments. It incorporates guidance developed by the National Computer Security Center to use password systems in national security computer systems.

By using the NSDD 145 mechanism for disseminating documents such as this, we can help to avoid duplication of efforts and achieve effective utilization of coherent, consistent practices for computer security throughout the Federal Government.

As explained by Mr. Brown, we believe that the Brooks Act, Public Law 89-306, already provides NBS with necessary authorities to address the problems highlighted by H.R. 2889.

I want to again thank the committee for its interest in our work and I would be happy to answer your questions.

[Mr. Burrows' prepared statement follows:]

U.S. DEPARTMENT OF COMMERCE

STATEMENT OF MR. JAMES H. BURROWS
DIRECTOR, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY
NATIONAL BUREAU OF STANDARDS
BEFORE THE SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY
COMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 18, 1985

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

Thank you for inviting me to speak to you today and for your interest in this critically important subject. The need for computer security has never been greater than it is today. The legislation that you are considering, H. R. 2889, takes note of the factors that contribute to this pressing need -- the government's dependence on computers, the scale of government computer operations, the widespread dispersal of personal computers throughout the government, and the valuable and sensitive information that is contained in government computer systems.

Rapidly changing technology and the escalating use of computers will continue to make computer security a high priority issue in the future. We see that it is impossible to return to manual methods once an organization adopts automated data processing methods. To achieve efficient information interchange, we must strive for standard, interoperable hardware and software systems. At the same time, however, widespread use will increase the vulnerability of our systems to external and internal threats.

To prevent serious accidents and intentional activities that cripple our ability to carry out data processing operations and to avoid compromise of sensitive information, we must stimulate an awareness for the need for computer security in managers and users of computer systems. This is the key element in a campaign to improve computer security, and this is the thrust of H. R. 2889. I believe that this legislation addresses clearly established needs for computer security research and for training the people who manage, use, and operate Federal government computers.

Training for computer security is going to be essential in tomorrow's computing environment. The reports last week about the high level of personal computer use in Federal agencies highlight the urgency of this need. Issuing directives to improve security will not be enough. Structured, organized, systematic training opportunities will be a must if the Federal government expects to exploit the use of advanced technology for improved staff productivity and reduced costs of government.

The legislation calls for the National Bureau of Standards (NBS) to conduct computer security research leading the development of technical procedures, practices, standards and guidelines for use in training. Many guides and reports that NBS has developed are already available and widely used for use in training programs. However, in order to deal with the urgency of the computer security problem as laid out in H. R. 2889, it will be necessary for NBS to expand greatly the kinds of materials it develops and to develop materials suitable for widely different needs. Computer security awareness programs must be available not only for the managers and users of automated information systems, but also for other agency personnel such as internal auditors, Inspectors General personnel, and budget analysts and managers. This will be essential to enable corrective actions to be proposed and implemented for information system development, operation, and modification.

These awareness programs and the renewed emphasis on computer security will also heighten the demand for timely products from NBS. Further, as new uses are made of computers and as new users become familiar with computer capabilities, new weaknesses will be exposed. Therefore, continuing attention to research and the development of effective protective methods will be needed.

The Institute for Computer Sciences and Technology at the National Bureau of Standards is currently carrying out a program of research in computer security areas. This program was started in 1972 as a component of our responsibilities under P.L. 89-306, the pioneering legislation authored by Chairman Brooks to improve the efficient and effective use of computers in the Federal government. Responsibility for developing computer security standards and guidelines is also specifically assigned to the Department of Commerce under OMB Circulars, and has been delegated to NBS. The Paperwork Reduction Act also provides additional legislative authority to carry out our program.

The problems that we are addressing are broad in scope and include many different hazards -- for example, physical damage to computers, accidents, destruction of data, theft of data and software, programming and data errors, omissions, and abuse of computing resources. While breaking into systems and computer crime are serious incidents, they are just one aspect of the problem. We are also concerned about the losses that result from processing incorrect data, from interruptions to data processing, and from lack of controls to prevent misuse of computers by authorized personnel. A vast amount of unclassified, but sensitive, information must be protected. This includes personal, proprietary, and other information protected under the Privacy and Freedom of Information Acts.

ICST's program is targetted to three principal objectives: computer integrity; this means the ability to prevent or detect unauthorized modification or destruction of computer information; confidentiality, the ability to prevent unauthorized disclosure of information; and availability, the ability to assure that processing resources are ready and waiting when needed. Failure to achieve these objectives in Federal government computing operations could result in undesirable events ranging from threats to national security to denial of benefits to citizens, loss of Government money and resources, human injury, or loss of life.

Under our legislative charter and policy directives, we develop management guides, test methods, performance measures, technical information and advice, guidelines, and standards. In developing our products and services we pay particular attention to the problems of Federal computer users and to the development of cost effective security methods that are appropriate to the information and systems to be protected. We also emphasize good preventive techniques because it is often more cost effective to avoid costly errors and accidents then to recoup after an expensive mistake. We have found that State and local governments, business, and industry users have problems similar to the Federal government's and that our technical products are used by the private sector as well as by the public sector. They are frequently used as the basis for training and education programs such as those conducted by the Small Business Administration and the Office of Personnel Management.

In the area of computer security and risk management, as well as in other program areas, we work closely with users in large and small organizations to learn about their experiences and their needs for technical and management solutions to their computer utilization problems. Because we are a small organization, we believe that the best way to achieve change is to work through other organizations. We sponsor, and participate in, conferences, workshops, and meetings to share information and to keep users and industry informed of our activities, as well as to learn what others are doing. We respond to requests for advice and consultation, we participate in training seminars to the extent that we can, and we provide direct technical assistance to Federal agencies on a reimbursable basis for limited number of projects that are related to our program.

I especially want to emphasize our work with the National Security Agency (NSA) and the National Computer Security Center (NCSC). NSA has conducted extensive research in the development of security technology for national defense applications. We are continually evaluating the applicability of these research activities to the civilian side of government and the private sector, so that we can transfer appropriate technology to the users who need it. Guest workers from NSA are working with ICST staff, and we maintain close staff contact on technical issues. We will be hosting the eighth national conference on computer security with DOD later this month. The conferences have been well attended by both government and industry participants.

We have cooperated with the General Accounting Office in their reviews and evaluation of agency computer security and have provided briefings and seminars on computer security to many Federal and State government organizations. We also participate in meetings sponsored by business and industry organizations to learn what they are doing and to make their good practices available to government users. Groups that we work with include EDP auditors, computer security professionals, internal auditors, universities, bankers, lawyers, and computer user groups.

As a result of our interactions with these groups, we are in a position to analyze user experiences and to identify best practices based on currently available technology. We have published a variety of reports, documents, guides, and studies conveying what we have learned. Through our contacts at many levels and with many organizations, we try to leverage our products so they reach a wide audience. For example, we are a clearinghouse of information that we have collected on computer security training opportunities, reading lists, and computer security services. This information is available electronically on a computer-based bulletin board.

We cooperate with business and industry to develop national and international consensus standards for computers and networks. We can do this effectively because of our knowledge of user and industry needs for standards and the position of trust that we have as objective participants in the standards process. Our goal is to stimulate the development of off-the-shelf commercial products that will expand choices, provide for interoperability of components and systems, and broaden opportunities for applications of new technology.

We are working with voluntary standards development groups sponsored by the American National Standards Institute, Institute of Electrical and

Electronics Engineers, the International Organization for Standardization, the American Bankers Association, and other national and international groups. We also participate with the National Communications Systems and the General Services Administration to develop Federal Standards for telecommunications.

Another important collaborative effort is our work with the Department of the Treasury to develop a policy to assure the integrity of electronic fund transfers. Last year Treasury issued a directive requiring the use of a voluntary standard for Financial Institution Message Authentication, to protect the billions of dollars that are transferred electronically every day. ICST was a major contributor to the standard, and to other voluntary standards developed for the private sector banking community.

The Treasury directive requires that all of its bureaus' EFT transactions be authenticated using data encryption techniques. Authentication is a process of coding and decoding significant phrases in a message to assure that it has been sent by an authorized party and has not been tampered with during transmission. ICST staff has been working with the voluntary standards community to draft a standard for protecting the secret keys that are used in coding and decoding messages. Automated key management techniques that were developed and patented by ICST staff are specified in this standard. Available on a license-free basis to organizations that want to use them, these techniques are being implemented in ICST's laboratory to help organizations test their products for compliance with the standard. A list of certified message authentication devices and techniques will be developed by Treasury with ICST and National Security Agency assistance.

ICST is working in conjunction with the National Security Agency (NSA) in developing proposed standards for data integrity and security in distributed computer networks. These efforts will focus on methods of securing data communications using data encryption techniques in a network of microcomputers. Commercially available software, protocols, and equipment will be used wherever possible. The network and primary security features will be unclassified, but will be designed to support more stringent security requirements for special applications.

Security of personal computers is currently under investigation. We recently issued a guide explaining security threats in the use of small computers and ways to reduce the risks. We are looking at a wide range of commercially available computer security devices for small systems to develop guidance for users in selecting cost effective security equipment.

We are participating in a joint project with the President's Council on Integrity and Efficiency to develop criteria for auditors to use in establishing their work plans for auditing for security and controls through out the life cycle of an automated information system. Specific guides and recommendations will be issued through this effort.

Security must be an integral part of overall systems planning. Therefore, we must be concerned about security in all of our technical activities, and we must address all aspects of computer system development and operations. This includes software systems, networks, storage media, and other hardware components. The weak link can appear anywhere in a complex system, and a comprehensive approach is needed to assure that strengths in one part of the system are not wiped out by weaknesses elsewhere.

As you know the Department of Commerce is one of the members of the National Telecommunications and Information Systems Security Committee established under National Security Decision Directive 145, and we have been participating in the Subcommittee on Automated Information Systems Security. A major focus is the development of definitions of sensitive, but unclassified, government or government-derived information which has an impact on national security.

We believe that we can contribute to the implementation of NSDD 145 which complements, but does not substitute for, our work. We expect to continue to issue Federal Information Processing Standards for automated information processing security under our current authorities. Those that are appropriate for issuance under NSDD 145 will be submitted for processing under the procedures that are being developed by the National Telecommunications and Information Security Committee. For example, Federal Information Processing Standard 112, Password Usage, is the first approved FIPS that will also be processed under the Directive. Its intended use includes protecting passwords in both the classified and unclassified information environments. It incorporates guidance developed by National Computer Security Center to use password systems in national security computer systems. By using the NSDD 145 mechanism for disseminating documents such as this, we can help to avoid duplication of efforts and achieve effective utilization of coherent, consistent practices for computer security throughout the Federal government.

As explained by Mr. Brown, we believe that the Brooks Act (P.L. 89-306) already provides NBS with necessary authorities to address the problems highlighted by H. R. 2889.

I thank the Committee for its interest in ICST's work, and I will be very happy to answer your questions.

Mr. **Brooks**. Thank you very much, Mr. Burrows.

Mr. Burrows, are additional resources over and above the current funding for the Institute for Computer Sciences required to accomplish the purposes of this bill, to implement this bill?

Mr. **Burrows**. I believe that the computer security program will need augmentation in order to meet the requirements of this bill. I am not sure they will occur immediately but in time as people demand products and technology shifts, and it becomes more available to every man in the street, the threats will become greater and more resources will have to be pushed into this area. Indeed to mount an awareness program, which I don't think we have today, new activity has to be started somewhere.

Mr. **Brooks**. You are now doing some of this work, right?

Mr. **Burrows**. That is correct.

Mr. **Brooks**. Under your current authority and appropriations?

Mr. **Burrows**. That is correct.

Mr. **Brooks**. Do you think to broaden that responsibility it might well take some additional funding, as we bring this problem to the public knowledge?

Mr. **Burrows**. Somebody has to mount the awareness program.

Mr. **Brooks**. Do you have an idea of what kind of funding that might be—in your personal opinion? What is your total funding? It isn't very much. What is it now roughly?

Mr. **Burrows**. For the total program we get from Congress for ICTS it is $9.6 million next year.

Mr. **Brooks**. $9.6 million?

Mr. **Burrows**. Yes.

Mr. **Brooks**. They couldn't even find that amount in the Defense Department. Do you know they found $37 billion more over there? Don't answer that. Don't get into that.

Mr. **Burrows**. Thank you. If they just would send me an old desk I would like that.

Mr. **Brooks**. $9.6 million doesn't sound like much unless you keep saying it over and over, of course, but to have an orderly phased progression of this effort would that take on the order of another $2 or $3 million perhaps?

Mr. **Burrows**. I think a phased program would have to be designed first before I could give you any indication of how much additional resources would have to go into security.

Mr. **Brooks**. The Institute's budget has been decreased or frozen over the last 5 years. Although the Commerce Department may have funded you, the OMB recommended it be frozen. Do you think it is possible for your current responsibilities to continue—much less additional work at that frozen level?

Mr. **Burrows**. I think it is clear the answer to that has to be no.

Mr. **Brooks**. Mr. Horton.

Mr. **Horton**. Thank you, Mr. Brooks.

Mr. Burrows, we are happy to have you before the committee and congratulate you on the job you have been doing. Have you found industry to be cooperative with the Institute in testing and setting standards as a result of those tests?

Mr. **Burrows**. I have found that the industry which pours a lot of money into the standards arena, much more than we do, has indeed in the last 5 years been working for, rather than against, standards which is what I think was the case in the 1970's.

They are beginning to recognize that no one owns the whole world, everybody has to play together, and that a common standard makes a larger market. Not everything is standard but the places where things have to go together they have to be standard or they don't work together.

They are moving in a direction to standardize those areas which are mostly the areas in which I work in order to enlarge the market and make sure they get part of it rather than be left out of it.

Mr. HORTON. Do you feel that the program such as the one that is conducted by the Institute could be carried out by any other governmental bodies or the private sector?

Mr. BURROWS. The total program?

Mr. HORTON. Yes.

Mr. BURROWS. No. I do not.

Mr. HORTON. There has been some indication that the Institute is not that healthy. What is your prognosis? Do you think it is going to be abolished? Do you think it is not a very well liked agency? What is your general attitude regarding what is going to happen to it?

Mr. BURROWS. That is a difficult problem. The indications I get from both industry and the Government are that our products are appreciated, industry is working with us in many of the areas to make sure that a combination of their work at home, and their design laboratory work, and work in the standards arena are nonconflicting in such a way that—they also work much more than we do in the standards arena.

But we just represent the Government needs in the standards arena and we try to be sure that standards get set.

Mr. HORTON. You are not having to look around the corner before you stick your neck around the corner and get your head cut off?

Mr. BURROWS. I haven't gotten that paranoid yet.

Mr. HORTON. Mr. Chairman, that is all I have.

Mr. BROOKS. Would it not be beneficial to have a closer association with the vendors and manufacturers, Mr. Burrows? To have a full discussion with them both on the technical aspects and the policy aspects of security from the standpoint of both the civilian agencies as well as the military, wouldn't it enhance everyone's interest to design more and better security measures into the new computers the Government buys from private industry? Wouldn't industry be able to translate that into better security for private business as well, which also runs a risk?

Mr. BURROWS. I think that the industry is very aware of the possibilities of compromise and other things in information systems. However, we don't build a product that costs more for a market that doesn't want to pay for it. Unless the awareness for the need of security is present in the private and public sector to a greater extent, I don't believe they will take a lot of time inventing new solutions to security problems.

I believe that work done at the National Computer Security Center and the work we do is attempting to get industry working in this security area but until an awareness program is out and the market develops for it, the solutions will not come from the technical side.

There are a lot of administrative problems which we have which—there are administrative ways to reduce the risk. But industry will not put anything in the product until they see a market. The market has to be developed.

Mr. **Brooks.** Well, the need is there. It is obvious.

Mr. **Burrows.** I certainly believe that. I am sorry——

Mr. **Brooks.** Amateur hackers can get into the Pentagon. If they can do that, it means that almost every business computer in the country would be subject to the same type of intrusion and that has always been my theory since we first started looking at computers that with the first—when the computer was as big as this room and had air-conditioning above it, below it, and inside it, and all around the edges.

Mr. **Burrows.** I remember them.

Mr. **Brooks.** They had 8K memories and that was great. Now you can buy a 64K card made in California for $2. I think IBM will sell them to you for about $160, always a reasonable place to acquire topflight information. But you know, even then—and I am not a computer scientist and don't pretend to be—it was quite obvious to everybody that the very people that could design these machines also knew where the weaknesses were and how to get into the machines. Since those who designed it knew how to get into the machines—if their mind can devise a way to get into it—there is always another scientific, mathematical brain that can also figure out a way to get into them. With the stage of computers that we have now, there are computers getting into other computers.

The hackers just program the computer to work, and work, and work until they break in, until they break a secret code and find a method of access to any number of computers.

So I think this problem is a menace to everybody who has a computer. If you have a business and somebody breaks into your computer and erases your vital records, you are in deep trouble. I don't mean it is a matter of worry to the Nation, it is just that your business is in deep trouble. You don't know who owes you, or who you owe, or what the status of your flow of materials might be, et cetera.

As for the Treasury Department, there are electronic transfers of funds both internationally and within this country. Someone could disrupt the entire country by erasing these records. Now, I know they have backups. However, I have backups in some of my installations, and backups take time to put into play and sometimes you haven't transferred everything you need into a backup capability.

I think that security is a major problem for any industry. It is a major problem in this country for business. It is a major problem for the civilian agencies. I include the Treasury Department and how much they are going to market for—whether they go to market for $50 billion every quarter just to handle the deficit or maybe another $80 billion for the rollovers. When they are going to go and how they are going to go to market all affects market price. Wouldn't it be just fascinating to know this information if you were in New York bidding on those funds? That is the danger in the civilian apsects of it.

There is computer material for defense, of course, which we don't want the Soviets to know. So I think security is a major problem and your efforts to bring that to public awareness and to do something about it I think would be very helpful. We thank you very much. We appreciate your being here.

Mr. Burrows. Thank you, sir.

Mr. Brooks. Our next witnesses are Donald C. Latham, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and Robert E. Rich, Deputy Director of the National Security Agency, accompanied by Walter Deeley, Deputy Director, Communications and Computer Security, National Security Agency; Elizabeth Rindskoph, General Counsel, National Security Agency; and Col. Joseph Greene, Assistant to the Director for Computer Security, National Security Agency.

Gentleman, your prepared statements will be made part of the hearing record and you are welcome to proceed. At an appropriate time we will close the meeting for any classified material you may wish to discuss.

STATEMENT OF DONALD C. LATHAM, ASSISTANT SECRETARY OF DEFENSE, COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE, DEPARTMENT OF DEFENSE

Mr. Latham. Thank you, Mr. Brooks.

I appreciate the opportunity to discuss this area with you today. We strongly support the encouragement and attention you have brought to this area of computer security. As you were just saying, it is a vital area and a very serious problem that we have been trying to cope with for sometime now.

We believe that we have a running start on it. We have in fact a very good cooperative effort between the National Bureau of Standards and the National Security Center, and things are actually in somewhat better shape than people would realize and we are moving on this.

The important point that was made by one of the witnesses is that there is blurring of the distinction between computers and telecommunications networks and what you are seeing is that a public switch network today that handles your telephone conversations actually has in it a large data processor. So we are actually addressing this problem and NSDD 145 addresses the problem of telecommunications and information security as a systems problem. That is the way we are approaching it.

Now you asked a question earlier to one of the witnesses about the cooperation with industry and how we are working it. I would say that industry is very cooperative in this area.

For example, the National Security Agency's Computer Security Center has developed a number of memorandums of understanding with large data processing companies so that we can work together with them on their products, including proprietary information which we will safeguard for them.

We have been having a series of breakfasts with the CEO's and senior people with large computer companies, describing what we are doing, asking them what they are doing in the way of developing safeguards, and asking for their support. We are encouraged by the initiatives they have taken on their own.

As the last witness mentioned, however, you must have a market if they are going to provide a product that they expect to sell that has some sort of computer security safeguard in it.

To that extent we have developed an improved product list in which the National Center has set up a series of criteria with NBS to evaluate computer systems as to the level of security they can actually provide and today the list is growing, it is not growing as rapidly as we would like, but there are a number of computer systems on the market today that provide varying degrees of security including up to the highest level we know how to generate, the so-called A-1 level.

We have at least one system certified to that level. So I would say industry is aware and they are working the problem including the application of computer security and telecommunications security to banking and other places.

In looking at the bill you propose we also agree with the testimony of the witness from Commerce that we think the bill is unnecessary in that existing statutes, and principally the earlier bills that you were so involved in, really provided enough of the wherewithal to carryout the intent of the proposed bill.

Actually in listening to some of the earlier witnesses I am not sure they understand the high degree of cooperation and interplay that exists today between NBS and the National Security Center at NSA.

We have jointly sponsored large symposiums, there is another one going on next month, over a 1,000 people usually attend, there is very detailed interplay between Commerce and the whole NSDD 145 structure.

In fact, the issue had come up earlier about what is the sensitive information and what is sensitive non-national-security-related information, what does it mean? The gentleman who actually wrote the proposed draft definition of that is Mr. Burrows, who is a member of the subcommittee of the NSDD 145 structure addressing this. We have promulgated a definition of what is sensitive national security related information that is unclassified and also a definition of sensitive non-national-security-related information.

We can make that available for part of the record for you as well as a copy of this draft proposal here that would put that in as a formal document in the Government.

[The draft proposal follows:]

NTISS Directive No.---
Date:

NATIONAL SECURITY SENSITIVE INFORMATION

Section I - Purpose

1. This directive establishes a definition for sensitive, unclassified, government or government-derived national security-related information requiring protection from unauthorized disclosure, alteration or destruction; this directive also assigns the responsibility to the heads of federal departments and agencies to identify their agency's data in accordance with the definitions established herein.

Section II - Applicability and Scope

2. This directive applies to government and government-derived information that is electronically stored, processed, transferred or communicated by federal departments and agencies, but does not apply to information that is classified for national security purposes under other national security directives and/or Executive Orders.

Section III - Authority

3. This directive, issued pursuant to National Security Decision Directive 145, National Policy on Telecommunications and Automated Information Systems Security, requires that systems handling sensitive, but unclassified, government or government-derived, information shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

Section IV - National Security Sensitive Information

4. This directive defines sensitive, unclassified national security-related information as separate and distinct from National Security Classified information; from non-national security-related sensitive information; and from public information; and establishes sensitive national security unclassified information as a category of information requiring protection.

5. The reader is referred to E.O. 12356, "National Security Information", dated 02 April 1982, for the definition of national security classified information.

FOR OFFICIAL USE ONLY

DRAFT

10 SEP 1985

6. Sensitive, Unclassified, Information.

a. OMB Circular A-71 (TM-1)(and its planned replacement) defines "sensitive data" as:

> "'Sensitive data' is data which requires a degree of protection due to the risk and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data)."

The term "sensitive data" is further defined to include records about individuals requiring protection under the Privacy Act, proprietary data, and data not releasable under the Freedom of Information Act, as well as agency data that affect the agency's mission. Information, although neither sensitive nor sensitive, national security-related in isolation, can become sensitive national security-related when taken in aggregate.

b. This directive partitions the definition of sensitive into two categories: sensitive, national security related; and sensitive, non-national security related.

(1) Sensitive, national security-related information is unclassified information the unauthorized disclosure, alteration or destruction of which could adversely affect the national security interest.

(2) Sensitive, non-national security-related information is unclassified information which requires protection from unauthorized disclosure, alteration or destruction to a degree proportional to the risk or magnitude of loss or harm.

7. Public information. This category of unclassified government or government-derived information may be disclosed to the public without restriction but may require protection against erroneous manipulation or alteration.

Section V - Responsibilities

8. Agency heads are responsible for determining which of their data falls within the category of information described in paragraph 6.b.(1), supra, and shall provide annually, or as requested, to the National Telecommunications and Information Systems Security Committee (NTISSC), a list of their agency systems which electronically process, store, transfer or communicate such information.

Mr. Latham. We need to clarify a few points that have been made about NSDD 145 because I am afraid some people who have been talking about it have not read it.

There are several points about NSDD 145 that have been misconstrued this morning for some reason. First of all, the NSDD 145 does not empower NSA as the Government's overseer of all civilian agencies nor allow them—NSA—to get into everybody's computers and tell them what to do. If you read NSDD 145 carefully, it absolutely does not do that.

In fact, it says in three different places in the NSDD that only "where appropriate" will there be assistance to the civil sector and wherever they want to play in this area.

There is a system security steering group chaired by the National Security Advisor to the President. Civil agencies such as Treasury are represented on that group. In addition, there is the National Telecommunications and Information Systems Security Committee, which I also chair and on that committee is not only Treasury but Commerce, Transportation, Energy, and many others, so the civil sector is very, very involved and very much active in this whole NSDD 145 structure.

Further, the NSDD calls out that the implementation of these security measures is the responsibility of the Federal departments and agencies, not the Director of NSA or DOD. So if Commerce, Treasury, Interior, or someone will be instituting some computer or telecommunications security initiative we can give them advice and provide them information, but it is up to them to implement it, not the Director of NSA. There is somewhat of a misunderstanding of the scope and the so-called threat to the civil agencies posed by NSDD 145.

It (NSDD 145) is in fact a cooperative program. It is a program in which we have found good cooperation with NBS and I think as I said earlier, we do not need additional legislation to carry out this vital mission.

Thank you.

[Mr. Latham's prepared statement follows:]

STATEMENT

BY

DONALD C. LATHAM

ASSISTANT SECRETARY OF DEFENSE

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

AND

CHAIRMAN

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CONCERNING H.R. 2889

BEFORE THE

SUBCOMMITTEE

ON LEGISLATION AND NATIONAL SECURITY

COMMITTEE ON GOVERNMENT OPERATIONS

UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 18, 1985

Mr. Chairman and members of the Subcommittee:

Thank you for this opportunity to testify on H.R. 2889, known as the "Computer Security Research and Training Act of 1985". This bill has the objectives of providing for a computer security research program within the National Bureau of Standards (NBS) and also providing for the training of Federal Employees who are involved in the management, operation, and use of automated information (AIS) systems. The efforts of this subcommittee are to be applauded as it carries out its investigation of the importance of the computer systems security problem to this nation and considers actions aimed at coming up with comprehensive remedies to this complex issue.

Today, I would like to address myself first to the general intent and overall purpose of the bill by providing perspectives, in my dual roles as both the Assistant Secretary of Defense for Command, Control and Communications and Chairman, National Telecommunications and Information Systems Security Committee (NTISSC), of the problems we face. Second, I would like to highlight possible areas of potential confusion in the bill requiring clarification so as not to impact adversely on existing Administration programs.

First, I wholeheartedly support the general intent of H.R. 2889 to provide for much needed support in the area of computer systems security training and education. All too often this is an area sorely overlooked and poorly funded because it is not glamorous. Also, as you are all too aware, the computer system security problem is extremely complex and solutions to the problem are made all the more difficult by continuing rapid advances in the state-of-the-art. The emerging use of supercomputers and the proliferation of local area networks are but two examples of technology that make the computer systems security problem a challenge that must be faced now. The problem is immense in scope and requirements for R&D are currently being defined. The shortage of highly qualified and trained professionals in computer systems security aggravates the problem. Any effort to try to assist in this endeavor is clearly welcome.

In this regard, I view the intent of H.R. 2889 as a positive although unnecessary step because we feel we have the necessary statutory authorities already with which to carry out an aggressive computer systems security program. The National Bureau of Standards has for some time been an important center of expertise in certain facets of computer systems security and we expect these efforts to continue. Let me quickly caveat my comments by saying that, to be truly effective, these additional NBS efforts must be further focused in the context of on-going efforts such as those which fall under National Security Decision Directive (NSDD-145) so as to avoid costly duplication of effort.

As Chairman of the NTISSC, I view as one of my key responsibilities making sure the problem of computer systems security is recognized by the public at-large as an important national issue. We have not done as good a job as we might have done in the past because we were not properly organized. The NTISSC structure now in being provides that organization and we are moving ahead with an aggressive awareness program in concert with similar initiatives being carried out by the NBS.

At its last meeting on 4 September 1985, the Subcommittee on Automated Information Systems security (SAISS), one of the two major subcommittees of the NTISSC, approved for issuance to the NTISSC a proposal to require education and training of federal departments and agencies. I expect the NTISSC to take up this proposal and make it a National Policy. In this regard, the National Computer Security Center (NCSC) at the National Security Agency (NSA) has begun development of training courses in AIS systems security for a DoD-sponsored awareness program. The NCSC will provide materials to other government, departments and agencies for awareners training.

Let me focus just a moment on some other DoD education and training efforts. We are developing guidelines which will make it easier to determine and specify the level of security that a system needs when generating requests for procurements or acquisitions. Also, we are in the process of issuing an instruction entitled, "DoD Trusted Computer System Evaluation Criteria", hereafter referred to as the Criteria, to assist in evaluating the effectiveness of safeguards for Defense applications. By the way, the SAISS adopted use of the Criteria on an interim one-year trial basis. Finally, the DoD is undertaking an ambitious computer vulnerability reporting program aimed at correcting security weaknesses in DoD computer systems. This effort should also be very useful for designing a national reporting program.

In my testimony for Mr. Glickman, Chairman of the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, on 27 June 1985, I indicated that a high priority item was trying to provide a working definition for what NSDD 145 defines as "sensitive" but unclassified government or government-derived information the loss of which could adversely affect the national security interest. Since that time, the SAISS has approved for issuance to the NTISSC a proposal for defining sensitive information. Specifically, it separates unclassified but sensitive information into two categories: sensitive national security-related; and sensitive non-national security-related. The purview of NSDD 145 is only for the former category.

Let me reiterate that NSDD-145 does not cover unclassified but sensitive non-national security-related information and therefore, it in no way restricts, controls, or manages the activities of other federal departments or agencies who have responsibilities in non-national security-related areas.

On the matter of research and development (R&D) responsibilities, the NBS has a well-developed program in the area of computer systems security. The NBS derives its responsibilities from the Brooks Act of 1965 (P.L. 89-306), the Privacy Act of 1974 (P.L. 93-579), and the Paperwork Reduction Act of 1980 (P.L. 96-511). We view these responsibilities as distinct both in intent and focus from those cited in NSDD-145. Again, NSDD-145 addresses only unclassified but sensitive national security-related and does not cover unclassified but sensitive non-national security-related information. More directly, privacy information, information on fraud, waste, and abuse, or proprietary data held by an agency is not covered by NSDD-145 dictates.

Let me quickly add that we don't intend to meddle in NBS authorities or responsibilities in these areas. Rather, we see the NBS efforts and those of other federal agencies under NSDD-145 as complementary and supportive of each other. Clearly, technical measures and techniques can apply equally well in many circumstances and technical interaction must be encouraged.

Indicative of the strong current relationship between the NBS and the DoD, is the high-level of cooperation between the NBS and the National Computer Security Center at NSA which is already impressive and growing. Specifically, they have jointly sponsored for the past eight years a National Computer Security Conference. This year's conference, scheduled from 29 September 1985 to 3 October 1985, will focus on mutual subjects of concern such as secure networks, verification, labelling, a profile of "hackers", and data base management security to name just a few. It will be attended by business, academia and government and allows for critical transfer of the results of the National Computer Security Center research and the NBS research throughout government and the private sector.

Important work is proceeding between NBS and the NCSC in the area of personal computers and office automation. In this regard, a Guideline on Password Management is being published by the NCSC and will become an appendix to the NBS Password Usage Standard already in existence. Additionally, the NBS has done impressive work in micro-computer and mini-computer systems security which the NCSC is using. As a final example, NBS and the NCSC is sponsoring a symposium on risk analysis to examine methodologies of mutual benefit. Again, these efforts represent the high degree of interaction between these two centers of expertise.

This cooperation must continue. While the staffs of both organizations are highly specialized, there is continuing reliance by NCSC staff on NBS Institute for Computer Sciences and Technology (ICST) staff expertise and vice-versa. In fact, two NSA employees currently are working at NBS with the purpose of transfering expertise to civilian users. This arrangement has worked remarkably well in the past and must be preserved.

Let me add that the NBS has taken an active role in the Subcommittee on Automated Information Systems Security (SAISS) of the NTISSC. The NBS member is the ICST Director.

As a final point on the issue of NSDD-145 and NBS responsibilities, NSDD-145 requires that NBS submit for NTISSC approval proposed computer systems security standards prior to their issuance as a Federal Information Processing System (FIPS) standard. Once again, this applies only to proposed standards where national security-related matters are concerned. Standards unrelated to national security are not covered. In this regard, it is anticipated that, Federal Information Processing Standard No. 112, Password Usage Standards, will be the first such standard processed under the NTISSC structure because it has application to both both unclassified and classified processing environments.

In closing, let me allay the fears of those who feel that NSDD-145 does in some way, shape, or form restricts current NBS research and development for standards-making efforts. NSDD-145 and the NBS programs stemming from the statutory base already mentioned are compatible and complementary efforts.

Computer systems security is a major challenge that needs all the available brainpower and resources this nation can muster. As such, let's move ahead together in the spirit of harmony and cooperation, not competition.

Accompanying me is Mr. Robert Rich, Deputy Director, NSA, who will further describe the activities of the Computer Security Center and other programs now being carried out by NSA in the areas of computer systems security awareness, education, training, and research and development.

Mr. Chairman, this concludes my prepared remarks. I would be happy to answer any questions that you or the Subcommittee have.

Mr. **Brooks**. Mr. Latham, thank you for your testimony. I want to say that on page 1 of your testimony, as submitted, I like the first sentence in the third paragraph. I would prefer that as a simple endorsement.

Mr. **Latham**. All right.

Mr. **Brooks**. You did continue, however. Would you precisely define unclassified but sensitive national security-related information? Give me specific examples of that type of information that may be in the civilian agencies or in the private sector?

Mr. **Latham**. OK.

Mr. **Brooks**. You know, funds transfers, money market funds.

Mr. **Latham**. Let me give you a definition and give you a couple examples. The way we have this draft definition it reads:

> Sensitive, non-national-security-related information is unclassified information which requires protection from unauthorized disclosure, alteration or destruction to a degree proportional to the risk or magnitude of loss or harm.

That is the current proposed definition.

Now in contrast, sensitive national security-related information unclassified is the "unauthorized disclosure, alteration or destruction of which could adversely affect the national security interest."

Now, what is the difference between those two? We have a program to automate the records in DOD hospitals. We are providing a level of security to that information because we believe patient's medical records would be sensitive non-national-security-information that is unclassified but which should not be publicly disclosed and we would protect.

So medical record information is covered. Some security information is another example. Funds transfers as you mention would be another example. By the way, the Treasury Department has instituted a protective measure on those fund transfer circuits between their various locations and they use cryptographic devices to protect those transfers.

An example of sensitive national security unclassified information in contrast could be information in our logistics system, such as, what is the level of certain types of spare parts, where are they, and things of that nature. So there is a clear distinction between the two types of information.

Mr. **Brooks**. What is your estimate of what it might cost the Federal Government to have adequate information security? Assuming you all agree that we ought to have it.

Mr. **Latham**. I absolutely agree we need to have information security. There will be additional resources required and it will take a considerable period of time to implement this. I don't have a number offhand, but one way to look at it is the following: Suppose you wanted to protect medical record information like we are in our new medical information system and they were to do this in another agency and even in the private sector? You could use what we call a C-1 level system, certified to the C-1 level. We believe the cost to do that at the system level is negligible to nonexistent.

It wouldn't cost you much of anything in terms of people, dollars or anything like that. In contrast to implement an A-1 level system, the highest we know how to do today that we would use on very sensitive command and control computer systems, might cost you 10 or 15 percent more measured in several ways, in dollars to buy the system, two, in terms of the need to buy an additional memory or additional speed in the computer to make up for the fact that putting in these computer security protections actually slows the system down because it has to do a number of checks and things like that. So the costs will vary.

The way I would approach it is to say it will be some percentage cost of each system, probably a number of 5 percent is good if you can look at it that way. I don't have a total number.

Mr. BROOKS. The Government spends roughly $30 billion a year on telecommunications.

Mr. LATHAM. I don't know that. If that is the case you——

Mr. BROOKS. Five percent is what, $1½ billion?

Mr. LATHAM. Somewhere in that neighborhood; yes. You are going to have to pay for communications security today, you really are going to have to pay for computer security and look at it as a delta cost to the system.

It is not as you know just some sort of hardware fix or software fix. It is a combination of procedures, people, training, and things of that nature. So the true cost is hard to actually come by.

Mr. BROOKS. Mr. Secretary, in your personal view, do you think the proposed bill should be modified to clearly delineate the roles of the National Security Agency and the National Bureau of Standards in the computer security area?

Mr. LATHAM. Yes, sir; in my personal view if you prevail and decide to go ahead with the bill I think there are a couple of relatively minor modifications that I would suggest you might want to consider to the bill.

One is in the area of defining what is sensitive information. The second is another sentence in one of the paragraphs to delineate and distinguish between this bill and NSDD 145. I don't think there is major surgery required.

Mr. BROOKS. Well, I thank you for that. Would DOD support a revitalized standards role within the National Bureau of Standards for Brooks Act applications?

Mr. LATHAM. That question is sort of like when is the last time you beat your wife, but it implies they are not doing it, not doing the job in the standards today. I would say in contrast I think they are. They can probably use additional funding. For example, Mr. Burrows didn't mention that in 1975 their budget was only $6 million and today it is a magnificent $9.6 so they hardly kept up with inflation.

They have been doing what they can with the money they have. They have been cooperating very much with the NSDD 145 structure and I would say that they could probably use additional funding, in my personal view to revitalize, if you wanted to call it that, their work.

Mr. BROOKS. I know they will appreciate that support.

Mr. LATHAM. Just don't expect me to write a check from DOD.

Mr. BROOKS. It isn't much.

Mr. LATHAM. We are so poor after you get through with us here——

Mr. BROOKS. DOD are just battles away whether they get $292 or $302 billion.

Mr. **Latham**. $302.5 billion is the number, sir, you know that.

Mr. **Brooks**. Yes; they don't have a prayer.

Where did they find that $37 billion that Senator D'Amato was talking about? Do you have another drawer out there? We ought to look in another drawer. There might be more.

Mr. **Latham**. I don't know but I doubt it.

Mr. **Brooks**. If DOD would just give a little of it, you know, to the National Bureau of Standards, it would help them a lot—just one of those little cubby holes, not a big drawer. Listen, in your view, might it be beneficial to establish a private sector advisory panel on computer security?

Mr. **Latham**. I am not sure we need that because we have one in existence already. We have established and have been active with them for the last 2 or 3 years, the National Telecommunications Advisory Committee which reports directly to the President and underneath that an advisory committee. We also have subworking groups and panels, largely from industry. There are 30 CEO's on the main advisory committee representing the 30 largest telecommunications, computer and aerospace companies.

Mr. **Brooks**. Where do they fit in on the evaluation of security?

Mr. **Latham**. What they have been doing for us for the last 2 or 3 years is addressing the national security emergency preparedness issues across telecommunications, imbedded computers, communicaitons satellites and things of that nature.

So we have in existence a mechanism today if we wanted to turn it up higher again so to speak and focus more on computer security, we can do that.

Mr. **Brooks**. I think we ought to turn that up a little because I feel we will never get a good security program unless the industry develops it.

Mr. **Latham**. I agree that they have to "come along" with us.

Mr. **Brooks**. The defense industry says they want to superimpose it on existing equipment, but that costs more money.

Mr. **Latham**. Yes; of course.

Mr. **Brooks**. You understand how that goes. If we bring them in in the first place and harass them and give them your problems, they may design that same security capability into their next generation machine that we buy. When the Government spends $30 billion a year, it should have an opportunity to have a substantial impact on that market.

Mr. **Latham**. Yes, sir. And as I said——

Mr. **Brooks**. We are a large customer. We write the specifications for what we want if we have enough sense—which is unlikely, because most of the real brains are in private industry. Tell me, are the best brains in industry because they pay them more money than they pay you or me?

Mr. **Latham**. That is right.

Mr. **Brooks**. So they have these brains and they can be very helpful and I don't think that they are necessarily unpatriotic. I think they want to do a good job for us and would if we bring them into the focus of it and put them to work. They will sell us the stuff anyhow.

Mr. **Latham**. Exactly.

Mr. **Brooks**. So let them sell you the stuff that best meets your needs.

Mr. **Latham**. And the market is developing, as I said earlier. If you go and talk to the IBM's and DEC's and others for the world, they are in fact implementing a computer security.

Mr. **Brooks**. There are other companies besides IBM, don't be narrow minded, though they do great work.

Mr. **Latham**. I said DEC.

Mr. **Brooks**. We have to be broadminded. We cannot have sole-source purchases.

Mr. **Latham**. That is right.

Mr. **Brooks**. We have to have an open marketplace.

Mr. **Latham**. I will supply for the record a list of all the companies.

[The information follows:]

There are 47 companies currently on the main advisory committee to the NSTAC:

Fairchild Industries
COMSAT
GE
Hughes Aircraft
MCI
Northern Telcom
Rockwell International
TRW
USTA
AT&T
CDC
GTE
IBM
Martin Marietta
Pacific Telcom
SDS
United Tech
Western Union
Bell Communications
Ford Aerospace
Harris Corp
ITT
Motorola
RCA
TRT
United Telecom
CSC

Three companies from the original 30 have dropped off of the advisory committee:

EDS
ROLM
GTE SPRINT

Mr. **Brooks**. Mr. Horton.

Mr. **Horton**. Thank you, Mr. Chairman.

I am a little bit confused about this. You probably heard the testimony of Mr. Socolar from GAO. As I understand it, Directive 145 gives the authority to the National Security Agency, if you will, to oversee this security or set the goal for it, which has to do with national defense. Now, the Bureau of Standards is not involved in that overall oversight.

Mr. **Latham**. Yes, they are.

Mr. **Horton**. You get them involved at a lower level?

Mr. **Latham**. No, at a higher level.

Mr. **Horton**. Where?

Mr. **Latham**. If you look at NSDD 145, it lays out a management structure from the top of the Government down. You have a steering committee that is chaired by the National Security Advisory to the President underneath. Then there is the committee which I chair that cuts across the entire Federal Government and included there is the Department of Commerce as a full member of the NTISSC. Commerce sets right with me as does the Energy Department, Transportation Department, and other civil agencies.

Mr. **Horton**. Is Mr. Burrows the one that sits there?

Mr. **Latham**. No, sir, he sits on one—there are two major subcommittees—he sits on one. NBS is represented through Commerce on the senior committee and NBS itself is on the subcommittee structure under that.

My committee is the policymaking committee subject to the guidance from the steering committee which Mr. MacFarland chairs. We develop the policy and work it across the Government as a group. We have met four times in the last year on the issue and we are working technical and policy issues. The national manager who is also the Director of NSA implements that policy. He is not the policymaker. I view NSDD 145 as a much more benign document than others appear to think it is in that we are somehow imposing the Director of NSA on the Secretary of the Treasury or some other agency.

Mr. **Horton**. Well, the Director of NSA literally has authority to look at this security issue of all computers throughout the Federal Government, right?

Mr. **Latham**. Well, what we have done is we have asked OMB and they issued a data call to the entire Federal Government looking at having them come back to us and telling us the status and what computers they have, what security they have on them and so on. So we are doing a survey.

Mr. **Horton**. I have no problem with that. I think it is a good idea to know where they are and have the information.

Mr. **Latham**. Yes, once we have determined that we can take certain actions. Another thing we have done is develop evaluation criteria which has been published and is being used to help people evaluate the level of protection in their systems.

The third thing is that we——

Mr. **Horton**. Can you hold there a second, in other words, for Defense agencies you would have a higher level I assume than you would for a civilian agency?

Mr. **Latham**. It might be, but let me give you an example. We might find in the Department of Defense that, for adequate protection of some set of remote terminals accessing a logistics network, a given level of protection, the C-1 level might be adequate.

That same level might be very adequate also in some civil agency trying to protect some related type of information in their agency. So it is not necessarily true that DOD automatically puts some very, very high and costly level of protection on something, unless it is needed.

Contrary to what the GAO representative said we—NBS and the DOD, do a risk assessment on every single one of these and you go in and you say, what kind of information is it, who has access to it, what level of security should the information be protected, and on that basis you make a determination as to what the system should be.

So we are not open ended on cost. We do a risk assessment as well. We can in fact give you an hour briefing on how we do the risk assessment. It is a carefully thought through systems engineering approach to decide what level of security you want on any given computer system.

Mr. **Horton**. On the question of level of security, how does the Institute fit into that?

Mr. **Latham**. The Institute fits in in that the R&D programs of NBS and the National Security Center are coordinated. We both know what each other is doing so there is not any duplication or we try to minimize that duplication.

They are fully aware of the criteria we developed and endorse that. We are working in sync across this area. They are developing standards to promulgate into the civil agencies and so on but NSA's computer center is working with them in fact and vice-versa to be sure that whatever standards we issue are applicable from top to bottom and not at odds with each other. So I think we are working in good sync.

Mr. **Horton**. Thank you very much.

Thank you very much, Mr. Chairman.

Mr. **Latham**. Thank you.

Mr. **Brooks**. Thank you, Mr. Secretary.

The next witness is Robert E. Rich, Deputy Director of the National Security Agency. I want to comment in advance that his Agency has generally been pretty responsive to the needs of this committee and I look forward to his statement. I have looked it over already, and thought it was a good statement given the guidelines they operate under—at least, I think the guts of it is.

We will put it all in the record. But I would just reiterate that I appreciate his comments that he doesn't believe new legislation is needed; agrees with us on our strenuous efforts to protect information undergoing electronic processes; and applauds the concerns displayed by the sponsors and shares their objectives to ensure the Nation's computer systems are designed to include effective security features.

He welcomes this opportunity to express OMB's views that they are against our bill. We thank you for your attention, but you do understand, that when the OMB doesn't want to add anything they put the screws to every agency when they submit their statements.

Some of you may not know that if you are running an agency and you want to come and testify, your statement has to be cleared not only by that agency with which you are associated but also by the OMB.

The OMB sits on high. They have a bunch of ghouls over there that look over all the agency statements and say, "You have to say you are not for it." If the statements don't damn the legislation too badly, then OMB says—of course, we don't think it is necessary but we applaud your efforts. You can read into that comment that really none of these people are dead set against the legislation. The agencies understand that we have to do something about it, but they can't come and say so or OMB would cut their heads off or maybe just their left hand, I don't know.

We are deeply appreciative of your statement, Mr. Rich.

Mr. RICH. Thank you, Mr. Chairman. If I could add one comment briefly, I would like to.

Mr. HORTON. I read your statement, too.

STATEMENT OF ROBERT E. RICH, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY, ACCOMPANIED BY WALTER DEELEY, DEPUTY DIRECTOR, COMMUNICATIONS AND COMPUTER SECURITY; ELIZABETH RINDSKOPH, GENERAL COUNSEL; AND COL. JOSEPH GREENE, ASSISTANT TO THE DIRECTOR FOR COMPUTER SECURITY

Mr. RICH. There has been, I think, a certain innuendo, Mr. Chairman, in some of these proceedings that there is maybe a kind of adversary attitude growing up between my Agency and the Bureau of Standards. I would just like to be clear that that is far from the case, and as Mr. Latham has suggested in this particular field that you have under consideration, we have a very close and useful relationship as we do in some other fields, so I would just like to clarify that.

Mr. BROOKS. I think the gentleman states the facts. I think that is true and I want to mention it. That is an outstanding example of the possibility of the National Security Agency, a portion of the Defense Department, cooperating in that particular field genuinely with a civilian agency, the Commerce Department, through the NBS.

It is to your credit. The Government will get the benefit of the expertise which you both have. I want to thank you very much.

[Mr. Rich's prepared statement follows:]

STATEMENT OF MR. ROBERT E. RICH

DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to testify regarding National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," and the objectives, structure, responsibilities, and accomplishments arising from the NSDD, as well as the provisions of enactment of H.R. 2889, entitled "The Computer Security Research and Training Act of 1985."

Our modern world is heavily dependent on telecommunications and data processing. Yet, for all our dependence on these disciplines and for all the developments in technology, much remains to be done to address all facets of telecommunications and computer security. The Subcommittee on Transportation, Aviation, and Materials of the Committee on Science and Technology only last year recommended that the Administration view computer security in the broadest possible terms; establish a central focus with wide agency participation; review policy and improve related federal programs; and increase the role of the federal government in influencing public sector awareness. NSDD 145 clearly is responsive to these concerns.

We believe the following recommendations cited in the most recent Biennial Report on the Status of Communications Security in the federal government are complementary to the Committee's findings:

- Improved planning, development and production to deliver more communications security (COMSEC) equipment sooner and at lower cost.

- Revitalization of the COMSEC policy-making structure to facilitate requirements definition, prioritization, and funding.

- Increased efforts to secure computerized data networks and associated office automation equipment.

Raising computer security awareness across the entire government and providing the training needed for the managers, computer operations professionals, and computer users is an enormous undertaking. A general plan for providing this training has been prepared by the National Computer Security Center and initial contacts have been made with both defense and civil agencies of the government encouraging their participation in the planning and execution of this training task.

National Security Decision Directive (NSDD) 145 was signed by President Reagan on September 17, 1984, as a direct response to the Biennial Report recommendations. This Directive provides a broad approach to both telecommunications security and information systems security, involving both civil and defense organizations in the national responsibility for protecting government information where it is most vulnerable to exploitation by our adversaries--during electrical processing or transmission. NSDD 145 has refocused the national communications security and computer security policy-making structures.

In NSA's view, NSDD 145 provides for the safeguarding from hostile exploitation of systems which process or communicate sensitive information. That information may be classified national security information or other sensitive national security, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest. The NSDD also directs the government to encourage, advise, and where appropriate, to assist the private sector to identify systems which handle sensitive non-government information of concern to national security, and to evaluate their vulnerability and suggest measures for their protection.

Under Executive Order 12333, the Secretary of Defense is the Executive Agent of the Government for Communications Security. NSDD 145 establishes a National Manager as the operating arm of the Executive Agent. The Director, NSA, is the National Manager. Selection of the Director, NSA, as the National Manager acknowledges the experience at NSA in the field of telecommunications security and cryptology--a capability not available elsewhere in government. In all this time, NSA has been the authority to which both government and private organizations have looked for advice and guidance on cryptographic security.

NSDD 145's consolidation of sensitive computer and telecommunications security under a government manager is in line with the trend in technology and management practice which already has led many organizations around the world to establish a single senior manager responsible for both fields. The military services, civil departments and agencies of the Government, and our NATO allies all reflect this trend. The Secretary of Defense as Executive Agent and the Director, NSA, as National Manager, respond to the direction of the Systems Security Steering Group. This group comprises cabinet members as well as the Director, OMB; it is chaired by the President's National Security Advisor. An interagency committee, the National Telecommunications and Information Systems Security Committee (NTISSC), provides interagency guidance and coordination. The Secretary of Commerce also is a member of the NTISSC. The National Manager provides the day-to-day management and administration of the government's efforts. The NSDD assigns specific tasks to other departments and agencies where they have expertise.

Among these, the National Bureau of Standards (NBS) is charged with the issuance of Federal Information Processing Standards; the Manager of the National Communications System is charged to issue Federal Telecommunications Standards, and the Director, OMB, is responsible for overseeing budgets.

Moreover, as a participant in the activities of the National Telecommunications and Information Systems Security Committee, a representative of the NBS acts as chairman of a working group which is tasked to define "sensitive" information. As the acknowledged expert on the concerns of the private sector, the NBS chairmanship assures that full consideration will be given to private industry's concerns in developing this definition.

The NBS, with their private sector experience in computer research and standards development, has also been invited to participate as a member of the Technical Review Group (TRG) of the National Computer Security Center. A mutually agreeable arrangement is being developed with the NBS to ensure their participation in meeting the obligations of the government under NSDD 145 to protect government information, and to assist the private sector in protecting their sensitive or proprietary information.

Under this arrangement, we expect that the NBS will directly participate in the National Manager's national computer security program planning and requirements development, and research and development for the private sector. NBS will serve as the liaison between the government and industry in using and applying the appropriate programs and technology resulting from the efforts of the National Manager, while NSA will concentrate on activities involving cryptography and implementing security beyond the A1-level. NSA's main relationship with the private sector will focus on bringing industrial assistance to bear on the major task of securing and protecting sensitive government computer data bases from foreign exploitation and from domestic communications security threats.

The NBS and NSA association has been complementary, cooperative, and mutually beneficial in computer security. Joint efforts by NSA and the NBS are ongoing or planned in the areas of developing risk analysis methodology; evaluating limited-function security products; planning and executing computer security research and development as well as computer security training and awareness activities; participating in network security methodology; and evaluating criteria development and network security protocols. NSA and the NBS regularly seek each other's assistance.

National Security Decision Directive 145, establishes the new National Policy on Telecommunications and Automated Information Systems Security, and highlights the need to improve the security of both telecommunications and automated information systems across the nation. In the year since President Reagan signed NSDD 145, we have made a strong beginning to involve federal departments and agencies in a cooperative attack on the existing shortcomings in our protection of classified and sensitive government information.

Turning to H.R. 2889, we believe that new legislative authority is not needed.

In conclusion, Mr. Chairman, we wholeheartedly agree that strenuous efforts to protect information undergoing electronic processing is urgently needed, and we applaud the concern displayed by the sponsors of H.R. 2889. We share their objective: to insure that the nation's computer systems are designed to include effective security features. We welcome this opportunity to express our views and thank you and your Committee for your attention.

Mr. Chairman, this concludes my prepared testimony. I will be pleased to answer any questions that you or the Committee may have.

Mr. Brooks. Now at this point in our hearing we expect to proceed with additional testimony from the DOD witnesses that will have to be delivered in closed session.

Prior to that, however, I ask unanimous consent to enter into the record statements by Mr. A.G.W. Jack Biddle, Jim Dray and Fred Wood of OTA, Allan Robert Adler, and the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers.

[See app. 2.]

Mr. Brooks. We have a vote on a bill on the floor. Consequently, the subcommittee will go into executive session and resume in executive session after we go vote.

I would ask the clerk to make sure that the persons returning to the committee room are all properly cleared. The committee will stand in recess until this vote is over.

[Whereupon, at 12 noon, the subcommittee recessed, then at 12:15 p.m. reconvened in executive session. At 1:05 p.m. the subcommittee adjourned, to reconvene subject to the call of the Chair.]

[Subcommittee note.—The executive session portion of this hearing will not be printed.]

APPENDIXES

APPENDIX 1.—NATIONAL SECURITY DECISION DIRECTIVE 145

National Security Decision Directive 145

September 17, 1984

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued.

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechnical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

12. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

13. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

APPENDIX 2.—STATEMENTS SUBMITTED FOR THE RECORD

STATEMENT OF
A.G.W. BIDDLE
PRESIDENT
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Mr. Chairman, members of the subcommittee, it is a privilege to present our Association's views on H.R. 2889, a bill to provide for a computer security research program within the National Bureau of Standards and to provide for training of Federal employees in the use and management of computer systems.

The approximately 70 member companies of CCIA have long been concerned with one of the main thrusts of H.R. 2889: the improvement of security in federal data processing installations and in the communication of data between Government computers. The private sector, no less than the public sector, has been shaken by revelations regarding unauthorized entry of ADP systems by so-called computer hackers. Moreover, all data processing installations face an even greater threat from employees who are armed with passwords and other knowledge that allow them to penetrate the installation's physical and electronic defenses. And the computer installations of the United States must withstand the determined efforts of unauthorized intruders to intercept a wide variety of U.S. electronic communications.

Unfortunately, studies by GAO and other organizations have consistently reported that the federal sector has not taken adequate steps to protect the security of its computer installations. The Government spends approximately $12 billion annually on data processing and telecommunications equipment. The General Services Administration has estimated that by the end of the 1980s, the Federal ADP inventory will include approximately 25,000 medium to large-scale computers and 500,000 microcomputers. Clearly, the protection of the data stored in and communicated through the Government's ADP inventory is a vital priority.

To achieve this end, H.R. 2889 proposes to establish a computer security research program to be conducted by the National Bureau of Standards. Among other goals, the program is required to determine the extent of vulnerability in Federal agency and contractor computers, and develop improved means of protection. If properly funded, this effort should increase the nation's security . As far as it goes, H.R. 2889 is a positive contribution to the protection of information in federal computers.

We are concerned that H.R. 2889 does not go far enough to address the security problem. Any effort to address that problem must also focus on the need to establish a coherent management structure for computer security within the executive branch. Congress has attempted to provide the basis for such a structure under Public Law 89-306, the Brooks Act and the Paperwork Reduction Act, Public Law 96-511. Those statutes, generally, give the responsibility to promulgate standards, including standards relating to computer security, to OMB and the Department of Commerce.

These agencies and particularly the Department of Commerce's National Bureau of Standards, have made significant contributions to the improvement of federal ADP security. Under the leadership of NBS, the federal government has implemented a data encryption standard which is now a mandatory requirement of many federal procurements. Although these agencies can be criticized for failing to give sufficient priority to security concerns, we believe that present statutes have laid the groundwork for a sound management structure. Unfortunately, the Executive Branch has taken actions which may undermine the statutory framework for security standards and policies. On September 17, 1984, President Reagan issued National Security Decision Directive (NSDD) 145. This directive has changed, by Executive Order, the system for promulgating ADP standards enacted by Congress. We believe that this effort is, in some critical respects, contrary to law. We also believe that other aspects of NSDD 145 raise serious questions regarding information policy that must be examined closely by the Congress before they become standard procedure for federal agencies. Any legislation to improve the security of federal ADP installations must resolve the problems created by NSDD 145.

As issued by President Reagan, NSDD 145 attempts to increase security for classified national security information, and certain, unspecified "other sensitive government national security information" by establishing four organizational components. The Systems Security Steering Group oversees NSDD 145 and is responsible for its implementation. It is chaired by the Assistant to the President for National Security Affairs and includes six department or agency heads. The National Telecommunications and Information Systems Security Committee (NTISSC) is under the direction of the Assistant Secretary of Defense (Comand, Control, Communications and Intelligence or C3I). This committee operates under the steering group and considers various technical and policy matters to implement the directive. Ten of the group's 22 members are from agencies of the Department of Defense. The third organizational component is the Executive Agent for Systems Security--i.e., the Secretary of Defense. The Secretary is charged with the duty to implement policies and procedures of the NTISSC and the Steering Group. The final organizational component set up by NSDD 145 is the National Manager for Telecommunications Security and Automated Information Systems Security who is designated as the Director of the National Security Agency.

Even a cursory glance at this organizational structure shows that it is heavily weighted toward the defense and intelligence communities. And under NSDD 145, these organizational components are given the authority to override the predominantly civil organizations who have been required by Congress to develop national standards. NSDD 145 specifically provides that the Executive Agent of the Government for Telecommunications and Information Systems Security--that is, the Secretary of Defense--shall have the power to, "Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive." The National Manager for Telecommunications Security and Automated Information Systems Security--the Director of NSA--is specifically empowered to, "Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security." (emphasis added).

This authority is in direct contravention of the Brooks Act, which gives final, standard-promulgation authority to the Secretary of Commerce. Under NSDD 145, the Director of NSA is given the power to review and approve all standards--including those issued by the Secretary of Commerce. In essence, the Secretary of Commerce's power to promulgate standards has been subordinated to the power of the intelligence community to review and approve any standard which arguably relates to computer security. Since any standard regarding the communication of data between computers or the storage of data in a computer could arguably relate to "security," NSA's powers under this directive are extremely broad.

We do not dispute that NSA possesses a vast amount of technical expertise regarding security and encryption which should be utilized in the promulgation of federal computer standards. We also do not dispute that the Secretary of Defense possesses broad powers to protect classified national security information. What is of concern to the computer industry is the significant expansion of the NSA and DOD into standards efforts which have previously been conducted in open forums that allow full expression of vendor and Government concerns.

The development of federal, ADP standards is vital to both the federal government as a user of computer resources and the computer industry itself. The Brooks Act cannily predicted in 1965 that without meaningful standards, the federal government will never achieve certain economies in the operation of computer resources. Without standards, large segments of the federal ADP inventory will remain unable to communicate with other sections of the same inventory. Programs which operate on one computer will not operate on the other. The lack of effective standards has already cost the federal government billions of dollars in conversion and other costs. Improved security is certainly one, important component of an effective standards program. However, it is not the only goal of the federal standards program. NSDD 145 improperly seeks to override the more balanced judgment of Congress that the responsibility for developing and implementing computer standards must occur outside the intelligence community, which as a result of its mission, can only be sensitive to some of the concerns which should underlie the expanded implementation of ADP standards.

Our position should not be construed as advocating a standards process which fails to utilize the enormous expertise of DOD and NSA in computer security. We believe that improved means should be found to utilize the expertise of those agencies. However, ultimate power to "review and approve" ADP standards--including standards which are applied to nonclassified information--must reside outside the defense and intelligence communities. Only in this manner can industry and government together form a working partnership to increase the use and scope of federal ADP standards. And it is only by allowing the Secretary of Commerce to continue to exercise his statutory power to review and approve standards that the standards process will comport with existing statutes.

Our second concern is that NSDD 145 gives DOD and the intelligence community vast and largely undefined power to shape national information policy. In this area as well, we do not dispute the need for DOD and NSA to develop policies and procedures for the safeguarding of national security, classified information. However, NSDD 145 goes much farther than the mere affirmation of DOD and NSA control over classified information. The directive also gives these agencies broad powers over nonclassified, "sensitive" information of both military and civilian federal agencies. NSDD 145 establishes a broad policy requiring protection of, "Systems handling other sensitive, but unclassified government or government-derived information, the loss of which could adversely affect the national security interest..." To implement this policy objective, the Director of NSA is given the power to, "Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques and information."

This new category of protected information may have boundaries, but they are only discernible to the authors of NSDD 145. Clearly, the loss of the data bases which record the Social Security entitlements of millions of citizens would create a massive problem of national concern. Possibly, under the vague rubric of NSDD 145, this data would constitute "sensitive" information. But Congress has never indicated any desire to give DOD, much less NSA, the power to control access to this "sensitive information." By establishing this new category of protected information, NSDD 145 comes close to giving DOD broad new powers to classify--and thereby deny access to--a vast amount of information which historically has been outside the scope of Defense control. We believe that such a major change in federal information policy should not be undertaken. And it should not even be attempted without the full consent and deliberation of Congress.

The potential scope of NSDD 145 is so broad that it can be used to justify broad intervention in national information policy by the Secretary of Defense and NSA. Who can even define the expansive terms by which the directive defines its jurisdiction? What is "sensitive" information? Can it include privately-owned and generated information? What is "government-derived information?" To what extent does this directive authorize the imposition of controls or procedures regarding the transfer of "sensitive" information between wholly private concerns--at least where the information is "government derived"?

These questions are not answered by the sweeping terms of NSDD 145. Until these and other questions raised by the directive are solved, the Government's efforts to achieve effective computer security will be impeded. As a result of NSDD 145, the Government's management of information security is divided between a management structure established by directive and a managment structure established by statute. There is no present mechanism for eradicating the contradictions between these two structures. We believe that H.R. 2889 should resolve these contradictions so that Government efforts to achieve effective computer security will not be stymied by contradictory management directives.

We also believe that in the last analysis, the Government's efforts to achieve effective security rest with the private sector. Unless manufacturers build and design systems which provide increased security, federal efforts to achieve such security will often be frustrated. Federal efforts to improve security should complement private standards efforts which are designed to meet security and other objectives. We are concerned that H.R. 2889 takes no steps to implement a key recommendation of a prior House study on computer security. In its April, 1984 report on Computer and Communications Security and Privacy, the Subcommittee on Transportation, Aviation and Materials of the House Committee on Science and Technology concluded that there was a need to certify that computer products actually met standards for improved security. We strongly support the Subcommittee's recommendation that :

> The private sector should be encouraged to develop a certification process (e.g. underwriters laboratories) and a voluntary standards program to give users information on the specific capability of a device or technique as well as to indicate the condition or environment that permits optimum functioning.

At a minimum, we would urge this Subcommittee to include language in its report which supports this objective. In the long run, a close partnership between Government and industry is essential to achieve meaningful standards for both enhanced security and to achieve the economies in information processing that can only be obtained through widespread implentation of ADP standards.

STATEMENT FOR THE RECORD

of
Jim Dray, Research Analyst
and
Fred Wood, Project Director

OFFICE OF TECHNOLOGY ASSESSMENT
UNITED STATES CONGRESS

BEFORE THE

SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY
COMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

HEARING ON H.R. 2889: THE COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

September 18, 1985

COMPUTER SECURITY POLICIES

This statement is based upon work being conducted as part of the OTA assessment of Federal Government Information Technology: Congressional Oversight and Civil Liberties, originally requested by the Senate Committee on Governmental Affairs and the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice. As part of this assessment, OTA is examining the Federal Government's computer security policies through a critical review of relevant literature and reports, interviews and discussions with cognizant Federal agency officials, and an OTA workshop on computer security issues (which brought together two dozen security experts both in and out of Government). This assessment is still in progress, and the results in draft form have not completed internal review nor have they been reviewed by OTA's Technology Assessment Board. Therefore, this statement is limited to a brief description of the trends and policy issues which OTA is examining. If the Committee desires, OTA will submit a complete statement to the Committee for the hearing record after the assessment is completed and reviewed by TAB.

In its assessment work to date, OTA has identified a number of trends and issues that are relevant to H.R. 2889, the Computer Security Research and Training Act of 1985, and National Security Decision Directive 145 (known as NSDD 145):

First, OTA is examining whether the threats to Federal information systems are increasing, thus prompting a need for policy action. It is difficult to precisely ascertain the level of urgency of information security problems for a variety of reasons, including: the wide variety of Government computer applications, the varying sensitivity of information in these machines, and the suspicion that many incidents of computer abuse are not widely known or discussed. Nevertheless, many experts have argued that the Nation faces fundamentally new levels of risks in information security because of:

-- increased use of communication networks to carry important Federal data;
-- increased computer literacy and sophistication on the part of would-be perpetrators of abuse;
-- increasing use within Federal agencies of microcomputers and decentralized data processing that moves Federal information out from under existing protections; and
-- increased dependency on data processing overall, which results in more critical Federal data in electronic form and exposed to information security problems.

Second, OTA is examining the historical pattern of Federal policies on information systems security, and the indicators of their relative success, in order to determine what kind of new policy action might be useful. Consistent with the Brooks Act mandate, in 1978 OMB issued Transmittal Memorandum #1 to its Circular A-71, requiring agencies to establish a computer security program. However, while there is some evidence that awareness of information security issues has improved in the past 5 to 10 years in the Federal

Government, there are also a great many critical reports by GAO and the agencies themselves that point to continuing information security problems. OMB has proposed a new circular which updates A-71.[*] The most recent policy change has been the issuance of National Security Decision Directive 145 by the White House in September, 1984. The directive establishes a joint military/civilian committee to guide national security-related information security government-wide (known as the NTISSC); sets the Secretary of Defense as Executive Agent; and makes the National Security Agency National Manager for this computer and telecommunications security program.

Third, OTA is examining the factors which may cause agencies to neglect computer security management, in order to assess how policy implementation can be made more effective. Among the factors that have been suggested by participants in OTA workshops are: 1) competition for resources in Federal programs may tend to squeeze out spending for a "latent" issue like security, in favor of programs more visibly responsive to agency missions; 2) a lack of awareness or motivation among agency personnel may hamper security efforts; and 3) in some cases, as noted by the GAO in their 1982 report in this area, there is an absence of clear guidance for the agencies on appropriate security measures.

Finally, OTA is examining NSDD 145 as a policy strategy, and how it fits into the framework of other policies on computer security. As a significant new piece of the Nation's information policy, the directive has important implications for success in achieving secure information systems, as well as for the relative balance of roles between the agencies which guide policy and provide a technical resource for information security -- in particular DOD,

---

[*] Federal Register, March 15, 1985.

NSA, OMB, GSA, and NBS. The proponents of NSDD 145 have stated that the enhanced oversight mechanism it provides will give the Government's information security the leadership it needs. On the other hand, a variety of experts, including some who testified at the June hearings on computer security,* have raised concerns that the directive puts the DOD and NSA in an unusual, controlling position on information policy issues affecting both military and civilian agencies; that the needs of military and civilian agencies for information security differ, and thus a military-oriented apparatus would not be helpful to many agencies; that the committees guiding the implementation of NSDD 145 operate in secret; and that the directive's jurisdiction, "information sensitive for national security reasons," is vague.

Critical Questions on NSDD 145

Responding to the Committee's specific interest in NSDD 145, OTA has identified the following questions as critical in assessing the implications of the directive and possible congressional policy options:

1) In testimony on June 27, Walter Deeley, deputy director of NSA for communications security, said that, "Once a department or agency head has chosen to spend money on telecommunications security or automated information systems security, the NSA, as National Manager, prescribes or approves which COMSEC [communications security] or COMPUSEC [computer security] technique, system or equipment will be used." Similarly, NSDD 145 gives the NSA authority to "review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security." What is the extent of NSA's control authority over civilian agencies' security measures for telecommunications and computers?

2) In his testimony in June, Donald Latham, assistant secretary of defense, implied that the ultimate definition of information sensitive for national security reasons might include everything from personnel records to crop

---

* U.S. House of Representatives, Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, Hearings on Computer Security Policies, June 27, 1985.

reports to air traffic control data. What exactly have NTISSC and its subcommittees done in attempting to define information sensitive for national security reasons? What approaches have they considered, and how broad will the ultimate definition should be? How broad will be too broad, and thus would be too costly and unworkable to implement? When and how will the definition be implemented?

3) OMB says the Government spends about $15 billion on computers and telecommunications, although because many costs (particularly in Defense and Intelligence) aren't included in that figure, the total is probably closer to twice that. How much will it cost beyond what the Federal Government is currently spending to have adequate information security, using different definitions of "sensitive for national security reasons"?

4) A key problem with existing security policy, as noted by the GAO and others, is the lack of coordination and cross-referencing among the various policies (e.g., NBS guidelines, GSA procurement regulations, OMB circulars), and legislative mandates (the Brooks Act, the Paperwork Reduction Act). NSDD 145 seems to add to the confusion. How can the directive and other policy mandates be modified to improve this situation?

5) NSA appears to be aiming toward a situation in which, in the cryptography area, the algorithms are secret and under direct NSA control. Obviously, some secrecy is important in the guarding of classified information. However, to what extent is it necessary for the policymaking process itself to be secret? What problems does this secrecy raise for the unclassified side of government and for private industry?

6) Currently, security is largely an "add-on" to information systems, so security measures can be prescribed somewhat independent of the information system itself. However, the most effective way to develop secure information systems is to include security concerns throughout the design, development, and operation of the system. And, in part as a result of the DOD Computer Security Center's efforts, computer vendors are increasingly building security features into computer hardware and software, making security an integral part of the product. Does that mean that in order to fulfill its roles of prescribing standards, reviewing and evaluating the security of Federal information systems, NSA will increasingly have to evaluate and approve the design of civilian information systems which handle national security information?

7) The Data Encryption Standard is an example of the way in which government standards can be very powerful in shaping commercial products and activities in the information security area. As communications security becomes increasingly important in the private sector, what are the implications of the standards developed and approved by NSA? Will NSA end up as the de facto standards-setter for the entire country in information security? Or will the commercial sector break away entirely from NSA standards because of their inherent secrecy or cost? If one goal, as stated in DOD and NSA testimony, is for industry to increase their expertise in developing secure products, does the inherent secrecy of the NSDD 145 process hinder that development and the ability of industry to meet the government's needs?

8) Is there a need for a stronger technical resource on the civilian side of

government for information that is sensitive for reasons other than national security (e.g., privacy)?

9) Does NSDD 145 effectively place DOD/NSA in a strong, central position with respect to Federal information policy, considering that its scope may be broad (depending on the definition of sensitive for national security reasons), and its impact on the civilian agencies and the commercial marketplace is liable to be very significant? What are the implications for national information policy of essentially further blurring distinctions between classified and unclassified information?

General Policy Options

OTA is addressing the issue areas and questions outlined above in order to assist the congress in evaluating possible action. In order to be most helpful to this Committee as it evaluates H.R. 2889 and NSDD 145, OTA has assembled a list of policy options related to the issues discussed above that appear to merit analysis.

1. Congress could enhance oversight of information security in agencies, if on the basis of OTA and other work it is determined that computer security is a serious and/or worsening problem. In addition to hearings focused exclusively on information security, such as those held by the House Subcommittee on Transportation, Aviation, and Materials, the various oversight committees in both houses could include information security as a regular component of their agency oversight hearings. Congress could also hold hearings on the willingness of information system vendors to provide appropriate security measures built into their products. One security expert consulted by OTA suggested that the visibility of congressional hearings might be the most effective way to motivate vendors to build in such security.*

2. Congress could change the budget procedures to provide more visibility

---

* R.H. Courtney, Jr., interview with OTA staff, July, 1985.

for computer and telecommunications security in agency budget requests, if the OTA and other studies determine that budget pressures are indeed squeezing out spending for security. Currently, agencies usually do not break out their expenditures for information security, making oversight and cross-agency comparisons difficult. Congress could request that agencies specify their expenditures for security (both for staff and as components of information system operating expenses) and/or that OMB conduct a special analysis on this topic. The advantage of this measure is that it would make oversight of information security easier; the disadvantage is the additional paperwork that it would generate for the agencies or OMB. As an alternative, Congress could request and examine the information security budgets that agencies will be submitting to the NTISSC, and could examine closely the portions of agencies' annual internal control reports (submitted under the Federal Managers' Financial Integrity Act of 1982) that relate to information security.

3. Congress could designate a central agency to provide support for computer and telecommunications security in the Federal agencies, if the answer to the question in #8, above, is that a further technical resource is needed. H.R. 2889 is one way to achieve such a goal. It formally designates the National Bureau of Standards as a lead agency to do background research and provide guidance on agency training in the area of information systems security. Such a measure could strengthen and clarify the technical resources for information systems security in the Government; and formally provide for research on the civilian side of Government, to supplement the substantial work already done in DOD and NSA.

4. Congress could increase the funds for NBS' work in information security whether or not it is formally designated as a lead technical resource agency.

5. Congress could continue with the status quo, if OTA or other studies determine either that information systems security problems are not urgent enough to warrant enhanced congressional attention, or that existing policy measures and technical resources are moving in the right direction to address the problem.

Options Specifically Relating to NSDD 145

1. Congress could maintain close oversight of the implementation of NSDD 145, if it agrees that the directive is an important new information policy document, and wishes to help shape the implementation of the policy. Congress could focus oversight hearings on the evolving definition of information sensitive for national security reasons, which defines the jurisdiction of the directive; the scope and degree of control exercised by DOD and NSA over both military and civilian agencies; the effectiveness of the new policy in promoting better information security; and the relation of NSDD 145 to OMB's Circular A-71 and its proposed revision, as well as other elements of national information policy, such as the Brooks Act and Paperwork Reduction Act.

2. Congress could codify part or all of NSDD 145 into law, if it wishes to ensure itself a role in shaping and overseeing this aspect of information policy. In the process, Congress could also clarify the relation of the directive to other laws (e.g., the Brooks Act and Paperwork Reduction Act) which establish roles for the central agencies in managing information security policy.

3. Congress could rework the structure and intent of NSDD 145, possibly in addition to codifying part or all of the directive into law, if the result of OTA and other work indicates that some of the concerns expressed about the

directive are indeed valid. If it wished to emphasize balance between the civilian and military agencies, Congress could, for example, modify those aspects of the directive that appear to give military agencies jurisdiction over civilian ones.

4. Congress could continue with the status quo, if OTA's and its own evaluation suggests that normal oversight procedures will provide a Congressional role in the implementation of NSDD 145 and that the directive is moving in the right direction.

Thank you for the opportunity to comment on this important subject.

Statement to the
Subcommittee on Legislation & National Security
of the
House Government Operations Committee
on behalf of
The Committee on Communications and Information Policy
of the
Institute of Electrical and Electronics Engineers

September 18, 1985

This testimony is submitted by the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is the world's largest engineering society, with nearly 260,000 members worldwide, 214,000 of whom live and work in the United States. Approximately 82% of our membership is employed in industry, 8% in academic institutions, and 10% in the various government laboratories and agencies. The IEEE Committee on Communications and Information Policy is vested with authority to develop the Institute's communications and information policy; and, once that policy is adopted by the Institute, our committee is one of the major mechanisms by which the policy is voiced in public.

IEEE endorses the purposes of H.R. 2889 and believes a wide-ranging research program on computer security should be conducted.

Various degrees of computer security may be provided, according to the nature of information requiring protection and the consequences of its compromise. A given degree of computer security requires several parallel approaches:

- Physical security of facilities
- Authorization of operating personnel
- Secure operational practices by such personnel
- Safeguards to access through software
- Safeguards to data through encryption

The greatest degree of computer security is required for activities related to the national security for which the National Security Agency has certain operational and advisory responsibilities. However, a less stringent degree of computer security may be acceptable for civil agencies of government, which deal with unclassified government information. In addition, the private sector has need for a similar degree of computer security.

We believe H.R. 2889 is well conceived because it uses the mission and competence of the National Bureau of Standards to address this problem. There is a need for (1) research applicable to the less stringent needs of civil agencies, (2) standardization of equipment and operational procedures that embody the results of such research, and (3) dissemination of such results to the private sector. The NBS, as a civilian agency, is better suited to this task than the NSA, which is primarily a military agency. Nevertheless, the NBS and the NSA should keep well coordinated so that the civilian aspects or computer security are compatible with the national security aspects.

Because today's hearing focusses on the broader topic of the security of government and non-government information and, in particular, the allocation of responsibilities by National Security Decision Directive 145, we would like to call your attention to Congressional testimony we have previously given on NSDD 145. On June 27, 1985, we commented on the dangers we see in implementing the Directive's rules for unclassified, sensitive, non-government information and private sector telecommunications and automated information systems. That testimony was delivered to a subcommittee of the House Science & Technology Committee.

This Directive (entitled "National Policy on Telecommunications & Automated Information Systems Security," issued September 17, 1984) deals with three distinct aspects of the subject: (1) classified information; (2) other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest; and (3) sensitive non-government information, the loss of which could also adversely affect national security.

We, too, recognize an increasing need to protect the transmission and processing of information sensitive with respect to the commercial or the national security interests of the United States. Yet, NSDD 145 raises certain questions for us. We have no comment on the protection of classified information, which is governed by existing law and Executive Order. Similarly, we have no comment on sensitive, unclassified government information, which may be protected as the government sees fit. Rather, this statement will address five issues that NSDD 145 seems to raise with respect to unclassified, sensitive, non-government information and private-sector telecommunications and automated information systems.

1. How will one define the scope and limits of various categories of unclassified, sensitive, non-government information without abridging the exchange of information throughout the private sector?
2. How far does the proposed identification of private sector systems that handle sensitive government and non-government information extend?
3. How may close coordination and information exchange between the private sector and the government in protection technology be established while avoiding restraints on technological initiatives and scientific communication that may be undertaken by private firms?
4. Does NSDD 145 contemplate approval and endorsement of research and development by the private sector apart from contractual arrangements?
5. Does NSDD 145 contemplate that private sector systems will be subject to evaluation and certification, and, if so, on a voluntary or mandatory basis?

The first issue deals with the content of information itself. The remaining ones deal with the characteristics of systems that contain or transmit information and the extent of government involvement with them.

IEEE is concerned first as to the feasibility, in actual practice, of attaining the objectives of NSDD 145 insofar as unclassified, non-government information is concerned. The difficulty centers around the identification of "sensitive information" and the subsequent measures necessary to deal with it. Indeed, in the event that the protective efforts of the Systems Security Steering Group should ultimately extend to enforcement measures that may involve regulation, restraint, and monitoring, we see a real possibility of collision with constitutional principles of individual privacy and freedom of speech.

Secondly, IEEE is concerned at the extent to which the implementation of NSDD 145 seems to reach into the operation of private sector activities and systems. As the reach increases, so will the difficulties of identifying and evaluating systems and of reviewing and endorsing research in the private sector. NSDD 145 does not set the scope and limits of its interaction with the private sector.

Thirdly, as to scientific and technical information, with which the IEEE is particularly concerned, the open dissemination of unclassified information is deemed crucial to the continued advancement of U.S. industry

Finally, given that the policies of NSDD 145 greatly impact the private sector, we are concerned that private interests are not represented in the proposed implementation procedures.

For these reasons IEEE recommends that the groups responsible for implementing NSDD 145 review the feasibility of, and exercise extreme restraint in, designating categories of sensitive, non-government information. Certainly there should be no effort to regulate or control any such category. These groups should also exercise extreme restraint in efforts to identify and bring about the protection of private-sector systems that handle non-government information. Activities should be limited to alerting the private sector to the problem and encouraging appropriate private action. We also strongly urge, in view of the nature of the problem, that there be substantial representation by knowledgeable experts from the private sector on the government committees implementing the Directive.

The remainder of this statement addresses the five issues more fully. In each of the following numbered paragraphs, we have first noted a particular provision of NSDD 145 that affects our organization, then identified an issue raised by the provision, and finally commented briefly on it.

1. Characterization of Unclassified, Sensitive, Non-government Information

   Provision: NSDD 145 provides that the Systems Security Steering Group shall "[i]dentify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information." [Section 4.a.(10)]

   Issue: The issue is how to define the scope and limits of these categories without abridgement of the exchange of information throughout the private sector.

   Comment: Although the objective of identifying such categories of sensitive non-government information with a view to protecting them may appear attractive to some, we believe that almost insuperable difficulties surround the task because of the great variety and pervasiveness of information flows within our society. The boundaries of any such categories are inevitably diffuse and cannot be characterized with precision. Thus there is a risk of casting too wide a net in carrying out this provision of NSDD 145. The provision may turn out to be, at worst, excessively intrusive and inhibitive and, at best, ineffectual. Indeed, experience with analogous efforts under a prior Presidential Directive did prove ineffectual.

2. Identification of Private-Sector Systems That Handle Sensitive Government and Non-government Information

   Provision: NSDD 145 provides that the National Telecommunications and Information Systems Security Committee shall "[s]ubmit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities" [Section 5.b.(3)] and "[i]dentify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures." [Section 5.b.(4)]

   Issue: The issue is how far this mandate extends into private sector systems. Presumably, the "established objectives" cited above embrace "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest." [Section 2.b.]

Comment: The mix and proliferation of private, commercial, government, and government-derived information is widespread throughout both the leased and the public switched networks. Therefore, it would be an extremely complex undertaking to identify individual commercial and private sector telecommunications circuits that handle sensitive non-government information. The government would have to rely on the full involvement of the private sector in this effort. The government would also have to provide assurances that its methods of identification are nonintrusive and in compliance with law.

3. Support for a Technical Base Within the Private Sector

Provision: NSDD 145 states that one of its objectives is to provide for "...support for a superior technical base within the private sector in areas which complement and enhance government capabilities" [Section 1.b.] and "...encouragement of private sector security initiatives." [Section 1.c.]

Issue: The issue is how to establish close coordination and information exchange between the private sector and the government in this technology while avoiding restraints on the technological initiatives and their applications that may be undertaken by the private sector.

Comment: We endorse the provision of technical support in this area as essential to national goals. However, experience with support for research and technology in other areas related to national security has shown that it is hard to manage the exchange of unclassified information in ways that satisfy both the government and the technical community. We advise against further restraints on unclassified information.

4. Approval and Endorsement of Research

Provision: NSDD 145 provides that the Executive Agent of the Government for Telecommunications and Information Systems Security and the National Manager for Telecommunications Security and Automated Information Systems Security shall "[c]onduct, approve, or endorse research and development of techniques and equipment for telecommunciations and automated information systems security for national security information." [Section 6.d. and Section 7.c.]

Issue: The issue is the extent to which the Executive Agent and the National Manager may approve research and development in the private sector. The context of the provisions seems to indicate that these functions are to be exercised only within the government for national security information. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector research is subject to approval.

Comment: Approval and endorsement of research in the private sector should occur only in connection with the normal contractual arrangements between the government and the performers of research. We urge the Executive Agent and the National Manager to make this point clear.

5. Evaluation and Certification of System Security

Provision: NSDD 145 provides that the National Manager for Telecommunciations Security and Automated Information Systems Security shall have authority to "[o]perate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems." [Section 7.h.]

Issue: The issue is whether evaluation and certification of private sector systems are contemplated, and, if so, whether on a voluntary or mandatory basis for the system operator. The context of the provision seems to indicate that these functions are to be exercised only within the government. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector systems are subject to evaluation and certification.

Comment: Mandatory evaluation and certification of private sector systems that do not handle classified information are inappropriate and raise problems of scope and limitations in view of the proliferation of systems and information noted under point (2) above. We urge the National Manager to clarify this point.

With your permission, we would like to request that the following attachments be made a part of your hearing record:

- IEEE letter to National Security Advisor, Robert C. McFarlane, datad June 27, 1985
- IEEE comments on Department of Energy Notice of Proposed Rulemaking (21 June 1985, 50 Federal Register 25722-25) dated August 29, 1985.

IEEE THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
345 EAST 47TH STREET, NEW YORK, N.Y. 10017, U.S.A. TELEX 236411

CHARLES A. ELDON
1985 PRESIDENT

PLEASE REPLY TO

June 27, 1985

Honorable Robert C. McFarlane
Assistant to the President
for National Security Affairs
The White House
Washington, D.C. 20500

Dear Mr. McFarlane:

We are writing to convey to you and the National Security Council the reaction of the Institute of Electrical and Electronics Engineers (IEEE) to a recent Presidential document that addresses the protection of sensitive information from hostile exploitation. The document is National Security Decision Directive (NSDD) 145, issued September 17, 1984.

The IEEE is the world's largest technical professional society with over 260,000 members in 157 countries. In the United States there are more than 214,000 members, working in industry, government, and academia.

We, too, recognize an increasing need to protect the transmission and processing of information sensitive with respect to the commercial or the national security interests of the United States. Yet NSDD 145 raises certain questions for us.

In each of the following numbered paragraphs, we have first noted a particular provision of NSDD 145 that affects our organization, then identified an issue raised by the provision, and finally commented briefly on it.

1. Characterization of Unclassified, Sensitive, Non-government Information

Provision: NSDD 145 provides that the Systems Security Steering Group shall "[i]dentify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information." [Section 4.a.(10)]

Issue: The issue is how to define the scope and limits of these categories without abridgement of the exchange of information throughout the private sector.

Comment: Although the objective of indentifying such categories of sensitive non-government information with a view to protecting them may appear attractive to some, we believe that almost insuperable difficulties surround the task because of the great variety and pervasiveness of information flow within our society. The boundaries of any such categories are inevitably diffuse and cannot be characterized with precision. Thus there is a risk of casting too wide a net in carrying out this provision of NSDD 145. The provision may turn out to be, at worst, excessively intrusive and inhibitive and, at best, ineffectual. Indeed, experience with analogous efforts under a prior Presidential Directive did prove ineffectual.

2. Indentification of Private-Sector Systems That Handle Sensitive Government and Non-government Information

Provision: NSDD 145 provides that the National Telecommunications and Information Systems Security Committee shall "[s]ubmit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities" [Section 5.b.(3)] and "[i]dentify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures." [Section 5.b.(4)]

Issue: The issue is how far this mandate extends into private sector systems. Presumably, the "established objectives" cited above embrace "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest..." [Section 2.b.]

Comment: The mix and proliferation of private, commercial, government, and government-derived information is widespread throughout both the leased and the public switched networks. Therefore, it would be an extremely complex undertaking to identify individual commercial and private sector telecommunications circuits that handle sensitive non-government information. The government would have to rely on the full involvement of the private sector in this effort. The government would also have to provide assurances that its methods of identification are nonintrusive and in compliance with law.

3. Support for a Technical Base Within the Private Sector

Provision: NSDD 145 states that one of its objectives is to provide for "...support for a superior technical base within the private sector in areas which complement and enhance government capabilities" [Section 1.b.] and "...encouragement of private sector security initiatives." [Section 1.c.]

Issue: The issue is how to establish close coordination and information exchange between the private sector and the government in this technology while avoiding restraints on the technological initiatives and their applications that may be undertaken by the private sector.

Comment: We endorse the provision of technical support in this area as essential to national goals. However, experience with support for research and technology in other areas related to national security has shown that it is hard to manage the exchange of unclassified information in ways that satisfy both the government and the technical community. We advise against further restraints on unclassified information.

4. Approval and Endorsement of Research

Provision: NSDD 145 provides that the Executive Agent of the Government for Telecommunications and Information Systems Security and the National Manager for Telecommunications Security and Automated Information Systems Security shall "[c]onduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information." [Section 6.d. and Section 7.c.]

Issue: The issue is the extent to which the Executive Agent and the National Manager may approve research and development in the private sector. The context of the provisions seems to indicate that these functions are to be exercised only within the government for national security information. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector research is subject to approval.

Comment: Approval and endorsement of research in the private sector should occur only in connection with the normal contractual arrangements between the government and the performers of research. We urge the Executive Agent and the National Manager to make this point clear.

5. Evaluation and Certification of System Security

Provision: NSDD 145 provides that the National Manager for Telecommunciations Security and Automated Information Systems Security shall have authority to "[o]perate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems." [Section 7.h.]

Issue: The issue is whether evaluation and certification of private sector systems are contemplated, and, if so, whether on a voluntary or mandatory basis for the system operator. The context of the provision seems to indicate that these functions are to be exercised only within the government. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector systems are subject to evaluation and certification.

Comment: Mandatory evaluation and certification of private sector systems that do not handle classified information are inappropriate and raise problems of scope and limitations in view of the proliferation of systems and information noted under point (2) above. We urge the National Manager to clarify this point.

Taking these issues as a whole, IEEE is concerned first as to the feasibility, in actual practice, of attaining the objectives of NSDD 145 insofar as unclassified, non-government information is concerned. The difficulty centers around the identification of "sensitive information" and the subsequent measures necessary to deal with it. Indeed, in the event that the protective efforts of the Systems Security Steering Group should ultimately extend to enforcement measures that may involve regulation, restraint, and monitoring, we see a real possibility of collision with constitutional principles of individual privacy and freedom of speech.

Secondly, IEEE is concerned at the extent to which the implementation of NSDD 145 seems to reach into the operation of private sector activities and systems. As the reach increases, so will the difficulties of identifying and evaluating systems and of reviewing and endorsing research in the private sector. NSDD 145 does not set the scope and limits of its interaction with the private sector.

Thirdly, as to scientific and technological information, with which the IEEE is particularly concerned, the open dissemination of unclassified information is deemed crucial to the continued advancement of U.S. industry.

Finally, given that the policies of NSDD 145 greatly impact the private sector, we are concerned that private interests are not represented in the proposed implementation procedures.

For these reasons, IEEE recommends that the groups responsible for implementing NSDD 145 review the feasibility of, and exercise extreme restraint in, designating categories of sensitive, non-government information. Certainly there should be no effort to regulate or control any such category. These groups should also exercise extreme restraint in efforts to identify and bring about the protection of private-sector systems that handle non-government information. Activities should be limited to alerting the private sector to the problem and encouraging appropriate private action. We also strongly urge, in view of the nature of the problem, that there be substantial representation by knowledgeable experts from the private sector on the government committees implementing the Directive.

For your information I enclose a copy of the statement of Dr. John M. Richardson on this subject on behalf of the IEEE, before the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, United State House of Representatives.

Sincerely,

Charles A Eldon

Charles A. Eldon

CAE/hef

Enclosure

1884 · 1984
A CENTURY OF ELECTRICAL PROGRESS

IEEE **UNITED STATES ACTIVITIES BOARD**
THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC

Russell C. Drew
Vice President
Professional Activities

PLEASE REPLY TO
1111 19th Street N.W. Suite [illegible]
Washington, DC 20036 U.S.A.
Telephone (202) 785 [illegible]
Telecopier (202) 785 [illegible]835

August 29, 1985

Department of Energy
Procurement Policy Branch
1000 Independence Avenue, S.W.
Washington, D.C. 20585
ATTENTION: Laura Bick (MA 421.1)

Dear Ms. Bick:

The following comments are submitted on behalf of the United States Activities Board of the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is the world's largest technical professional society, with nearly 260,000 members worldwide, 215,000 of whom live and work in the United States. Approximately 82% of our membership is employed in industry, 8% in academic institutions, and 10% in the various government laboratories and agencies. The U.S. Activities Board provides a forum for developing public policy positions on behalf of these members.

Our comments are directed to the Department of Energy's Notice of Proposed Rulemaking (21 June 1985, 50 Federal Register 25722-25) to amend the DOE Acquistion Regulation by establishing procedures for safeguarding sensitive unclassified information within industry.

During recent months the Institute's efforts at minimizing the degree of controls over unclassified scientific/technical information have taken the form of communications with the Secretary of Defense, testimony to a Congressional Committee, and a letter to the President's National Security Adviser. A copy of the IEEE President's letter to Robert C. McFarlane (dated June 27, 1985) on this topic is enclosed.

In so far as the proposed DOE regulation is concerned, we offer the following comments.

- IEEE is affected by this notice of proposed rulemaking (NPRM) because many thousands of its members are employees of firms that are contractors to the U.S. Department of Energy (DOE).
- The NPRM deals with information, telecommunications, and computers, fields in which IEEE members work.
- The NPRM deals with "DOE sensitive unclassified data stored in computer systems." This topic is a subset of sensitive, unclassified government or government-derived information, for the protection of which National Security Decision Directive (NSDD) 145 (issued by the President on September 17, 1984) is trying to develop a uniform government-wide approach.

The proposed rule is deficient in the following respects:

A. Uncoordinated action by DOE (and other agencies that may similarly act) in response to a problem that is already recognized as government-wide will proliferate disparate rules. DOE should wait until guidance is available from the level of the Assistant to the President for National Security Affairs, who serves as the chairman of the Systems Security Steering Group, established by NSDD 145.

B. "Sensitive unclassified data" is apparently left to officials of DOE to define on a case-by-case basis, without uniform guidance. Disparate interpretations of the meaning of this term will lead to nonuniformity, inequity, and confusion of application.

C. "Sensitive computer or telecommunications systems" are defined in terms of the inadequate concept of "sensitive unclassified data," or else in terms of the equally inadequate concept of "risk and magnitude of loss or harm that could result from improper operation." Disparate interpretations of the meaning of this term will also lead to nonuniformity, inequity, and confusion of application.

D. The proposed screening of personnel is insufficient of itself to achieve the desired protection. Other measures, such as physical security and encryption, should be considered in a coordinated approach to the problem.

E. The proposed screening of personnel is to be done in a perfunctory manner, without uniform guidelines or quality control. Nevertheless, the screening will become tantamount to some sort of "clearance;" if an individual fails to pass such an inadequately controlled clearance process, his rights to privacy, equal employment opportunity, merit promotion, and the like could be wrongfully abridged.

F. The rule, by placing additional impediments to the flow of unclassified technical information, will act generally to depress U.S. technological progress.

- IEEE opposes the proposed rule because of the deficiencies noted and favors its withdrawal.

In conclusion, we believe the sweep of the proposed rule is so broad as to embrace virtually all information in a DOE contractor's records and files. The protection of this unclassified information is to be carried out without statutory guidelines or government-wide guidance. If the information in question is vital to the national security, it should be classified and subject to control under procedures that are understood by the government and by the private sector as well. It goes without saying that classification, if applied, should be at the lowest appropriate level.

Sincerely yours,

Russell C. Drew

RCD/hef
Attachment

STATEMENT SUBMITTED FOR THE RECORD

By

ALLAN ROBERT ADLER
LEGISLATIVE COUNSEL
AMERICAN CIVIL LIBERTIES UNION

As requested by Subcommittee staff, the following statement concerning H.R. 2889, the proposed Computer Security Research and Training Act of 1985, is submitted for the hearing record on behalf of the American Civil Liberties Union:

It is no secret that increasing reports of computer-related fraud and abuse, together with detailed press accounts of the alleged espionage activities of present and former members of the military and intelligence establishments, have generated broad new concerns about the ability to protect telecommunications and automated information systems, in both the public and private sectors, against serious threats of exploitation and compromise.

The ACLU is sympathetic to these concerns because it has long been a champion of both the public's right to obtain necessary information from the Government, and the individual's right to protect his or her personal privacy from unwarranted intrusion or exposure by the Government. Although these vital interests in openness and confidentiality can often appear in conflict, the ACLU believes that neither can properly be served where a generalized perception of systemic information security weaknesses undermines routine assurances of effective protection for legitimate confidentiality interests and leads to overreactive remedial programs that could result in unnecessary and undesirable new secrecy practices.

As members of the Government Operations Committee well know, numerous proposals and pronouncements of the Reagan

Administration over the past four and one-half years have demonstrated its firm inclination to view all government information policies through the dark, uneven filter of what it broadly defines as "national security interests." President Reagan's National Security Decision Directive 145 concerning National Policy on Telecommunications and Automated Information Systems Security is the most recent and perhaps most disturbing manifestation of this narrow view.

In NSDD 145, the White House is pursuing an aggressively "comprehensive and coordinated approach" to telecommunications and automated information systems (T&AIS) security issues that casts its "Objectives" and "Policies" in deliberately vague terms of "National Security" interests, while attempting to meld civilian systems that handle nonclassified information in both the public and private sector together with classified national security information systems of the military and intelligence establishment to create a seamless "national security interest" for which overall responsibility is placed in the hands of the National Security Agency.

While the ACLU understands the Administration's apparent desire to avoid piecemeal security policy-making, and would not quarrel with its choice of NSA as the lead agency for security policy in connection with classified national security information systems, we read NSDD 145 and its designation of the Director of NSA as the "National Manager for Telecommunications and Automated Information Systems Security" as mandating an unprecedented, unwise and uncheckable primacy of the Nation's national security apparatus in information policy -- an area where the balanced consideration of values other than "security" is of paramount importance to our system of government.

The ACLU's concerns are based upon our reading of NSA's authority under NSDD 145; the implications of such authority in light of NSA's primary mission; and, the absence of a broad contrapuntal role for non-national security elements of the Executive Branch. Our conclusions on these matters, or, more precisely, the issues that we raise, point to the need for coherent Congressional involvement and direction in the program embodied by NSDD 145 so that improvements in T&AIS security are not purchased at the expense of an informed public and protections for individual personal privacy.

NSA Authority As "National Manager" Under NSDD 145

In sweeping terms, NSDD 145 designates the Director of NSA as "the government focal point" for T&AIS security policy, Sec.7.b., with authority to "review and approve all standards, techniques, systems and equipment" for T&AIS security, Sec.7.d.; "assess the overall security posture and disseminate information on hostile threats" to T&AIS security, Sec.7.g.; "prescribe the minimum standards, methods and procedures for protecting" T&AIS, Sec.7.i.; and, "review and assess annually" the T&AIS security programs and budgets of all agencies and departments of the government, Sec.7.j.

The scope of its authority to enter directly into the T&AIS

operations of all federal agencies and departments is broad in its literal terms and subject to expansion through its ambiguity. In Sec.7.a., the National Manager is granted authority to "examine government [T&AIS] and evaluate their vulnerability to hostile interception and exploitation," if necessary by means which may include "monitoring of official telecommunications."

Neither the reasons for, nor the meaning of, this power to "examine" agency T&AIS first hand is explained.

The NSA is also authorized to "request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned" to the National Manager. Sec.7.1. For their part, the heads of federal departments and agencies are ordered to "provide to... the National Manager... such information as may be required to discharge responsibilities assigned" to that office. Sec.8.c.

Finally, NSA's ability to influence the overall program is enhanced by the requirement that it provide "facilities and support" to, as well as staff to the "permanent secretariat" of, the National Telecommunications and Information Systems Security Committee (NTISSC) -- the umbrella group of specified agency representatives charged with development of "such specific operating policies, objectives, and priorities as may be required to implement" NSDD 145. Sec.5.d.

NSA influence in the NTISSC could have profound implications both inside and outside the federal government if concentrated with respect to the NTISSC's duty to "identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures." Sec.7.b.4.

Issues Raised By NSA's Authority and Other Aspects of NSDD 145

The pervasive theory of NSDD 145, which underscores ACLU concerns about the authority delegated to the NSA, is a view of "national security information" that reaches far beyond President Reagan's Executive Order 12356 on Classification to encompass a seemingly unbounded range of non-classified information in civilian T&AIS operations of both the public and private sector.

The effort to embrace security against T&AIS threats to "private or proprietary information of US persons and businesses" from "criminal elements", "terrorist groups", and "foreign exploitation" — along with the obviously appropriate concern for compromise of classified information by "hostile intelligence services" — has led the drafters of NSDD 145 to indulge the Administration's already disturbing penchant toward secrecy by presuming a need and authority for expansion of the universe of information properly subject to government security controls.

This awkward but determined straining of the "national security" rubric beyond its recognized limits is evident in repeated vague references to "sensitive" information and in the statement that "[s]uch information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate."

Moreover, its mischievous potential in blurring established laws and policies is manifest in the unclear policy distinction drawn between the indication that "classified national security information" shall be secured "by such means as are necessary to prevent compromise and exploitation," while "other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security." Sec.2.b.

The Administration's efforts to expand the category of "national security information" were not well received when they were entertained in the context of the drafting of President Reagan's Executive Order 12356 on Classification. New initiatives to achieve the same results through indirect policies should be even more forcefully rejected, especially at a time when it is clear that the Government is already attempting to protect far too much information "in the interest of national security." What do the terms used in NSDD 145 mean? What kind of "sensitive" information is at issue? If this information is in the private sector, is it privately-owned and generated? What is "government-derived information?"

These questions, based upon NSDD 145's broad yet ambiguous perspective on what kinds of information require the special T&AIS security expertise of the national security establishment, lead directly to a related inquiry about the impact on policies and operations in the civilian private and public sectors that may result from making the NSA the "government focal point" for implementation of NSDD 145.

It is not necessary to recite the litany of unlawful and improper NSA activities disclosed in Congressional hearings of the mid-1970s; the wholesale violation of the privacy rights of hundreds of thousands of Americans in the sweeping "Watch List" program known as Operation Minaret and the acquisition of millions of private cable communications under Operation Shamrock are a well-known part of an historical record of intelligence agency abuses that led to the creation of Congressional oversight committees, the enactment of specific statutory authorities such as the Foreign Intelligence Surveillance Act, and an ongoing effort to instill accountability into the intelligence process.

Although NSA still lacks a legislative charter and is still very much an executive creation whose activities are cloaked in extraordinary secrecy, it is not necessary to impute to NSA any residual lawlessness or "bad faith" motivation to question the wisdom of its designated role in NSDD 145's scheme for a "comprehensive and coordinated approach" toward T&AIS security throughout the federal government and the private sector as well. Assuming the best intentions on NSA's part, it still must be asked:

* Do NSA's priorities within the military/intelligence establishment inherently conflict with its role as "focal point" for T&AIS security for all government agencies and the private sector under NSDD 145?

* Will its policies in its role as National Manager be reflective of its primary military/intelligence mission, or will its advice be measured to lesser security needs?

* Will NSA's job-related disposition toward secrecy lead it to perform its duties under NSDD 145 with the same avoidance of public scrutiny that marks its day-to-day performance of its primary responsibilities?

* Is NSA's expertise perhaps too arcane for the actual needs of most non-national security agencies, in the sense that the best security programs might well be developed by those in each agency who are most familiar with that particular agency's systems and responsibilities?

It is clear that NSA itself cannot reasonably be expected to insure that considerations for open government and personal privacy are carefully balanced against perceived exploitation threats in devising sound T&AIS security policy; given the "national security" mindset that imbues NSDD 145, it is equally clear that the Directive offers no other source for such input within the the Executive Branch. This is perhaps just as well, since most advocates of these important values would be hard-pressed to recommend an Executive office, agency or department that has exhibited the ability or desire to effectively represent these interests in recent years.

H.R. 2889 would mitigate some of these concerns by creating a statutory mandate for the National Bureau of Standards to take the lead in developing and implementing a computer security research and training program for the Federal Government. But H.R. 2889 does not go far enough to address the challenge embodied in NSDD 145.

As Chairman Jack Brooks cogently argued in his testimony last June before the House Science and Technology Subcommittee on Transportation, Aviation and Materials, NSDD 145 flies in the face of statutory mandates giving OMB, GSA, and the Department of Commerce responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security. With implementation of NSDD 145 already underway, a Congressional response limited to enactment of H.R. 2889 will be too little and too late to regain the legislative prerogative for setting national policy on such an important set of issues.

Only the direct involvement of Congress can insure that openness and personal privacy considerations are given their full due in the development of T&AIS security policy. This is not, of course, an unusual role for Congress in light of its enactment of the Freedom of Information Act and the Privacy Act of 1974 -- measures aimed, respectively, at restricting Executive Branch discretion in denying public access to agency records and maintaining records in violation of an individual's right to personal privacy.

Only the direct and immediate intervention of Congress can ensure that the steps already taken and planned by Executive officials to implement NSDD 145 do not preempt the active and open involvement of the broadest spectrum of government agency and private sector interests, as well as essential Congressional legislative and oversight roles, in the formulation of national

T&AIS security policies.

As a first step, Congress should establish a statutory basis for the program set forth in NSDD 145. This would provide the necessary foundation for coordinating legislative and oversight functions with a directed scheme of Executive activities designed to achieve designated goals for the development of security policy. To the extent that the National Security Agency would continue to play a central role in the program, Congress should enact a legislative charter for that agency which clearly delineates NSA's primary duties and responsibilities.

It may, however, require a new Congressional mechanism to deal coherently with the issues presented by NSDD 145. Recognition that T&AIS security policy reaches beyond the national security characterizations that artificially bind them in NSDD 145 to embrace a whole panoply of information and privacy issues brings with it the realization that these diverse but related issues are currently scattered among the jurisdictions of numerous committees and subcommittees in both houses of Congress. The Judiciary, Government Operations, and Intelligence committees of the House and Senate, together with other individual committees in both bodies, each have responsibilities for some aspect of the Government's information and privacy policies, but have shown no inclination or ability to coordinate their consideration of related issues.

It may now be time for Congress to create a Select Committee on Information which can, in the words of NSDD 145, take a "comprehensive and coordinated approach" to information and privacy policies. Congress cannot ignore NSDD 145, and it can find it a useful impetus for bringing order to its own "houses" for consideration of information and privacy issues in the face of current and future technological developments.

○